Universidad Nacional Autónoma de México

Facultad de Ingeniería

"Implementación de un enlace WAN con capacidad para transmitir voz, video y datos sobre el protocolo IP, mediante el uso de la tecnología WiMAX"

T E S I S

QUE PARA OBTENER EL TÍTULO DE:

INGENIERO EN TELECOMUNICACIONES

P R E S E N T A N:

OLIVA ANDON ULISES

SANTILLÁN GUERRERO JOSÉ ANTONIO

ASESOR:
Dr. VÍCTOR RANGEL LICEA

Octubre 2012

Agradecimientos

A nuestras familias por el apoyo incondicional que siempre nos dieron. Externamos el más sincero y eterno agradecimiento por ese apoyo que perpetuamente nos han brindado y gracias al cual hemos logrado terminar nuestra carrera profesional, que es para nosotros la mejor de las herencias.

A nuestros maestros que día a día forjaron en nosotros las habilidades y actitudes que nos permitieron desarrollar nuestra tesis.

Con un infinitito agradecimiento a nuestra querida UNAM por permitirnos vivir una de nuestras mejores etapas de nuestra vida; con especial agradecimiento a nuestra Facultad de Ingeniería la cual nos ha dado las herramientas que nos servirán tanto en el ámbito profesional como académico.

Reconocimientos

Gracias a la DGAPA-UNAM por el apoyo otorgado para la realización de este trabajo a través del proyecto PAPIIT IN108910 “Diseño de algoritmos de reservación de capa cruzada en redes móviles y mesh de banda ancha”.

Gracias al CONACYT por el apoyo brindado a través del proyecto 105279 “Diseño de técnicas de reservación de capacidad de redes BWA móviles”

ÍNDICE

CAPÍTULO I *13*

Antecedentes *13*

1.1 Introducción **13**

1.2 Breve historia del desarrollo de las redes de computadoras. **14**

1.3 Definición del problema **16**

1.4 Objetivos **16**

1.5 Método **16**

1.5 Estructura de la tesis **17**

CAPÍTULO II *18*

Estándares y protocolos empleados *18*

2.1 Modelo OSI **19**

2.1.2 Breve explicación de las capas del modelo OSI 20

2.2 Estándar 802.16-2004, tecnologías WiMAX **22**

2.2.1 Evolución del estándar IEEE 802.16-2009 23

2.2.2 Subcapa MAC 25

2.2.2.1 Subcapa de convergencia para servicios específicos CS (ATM o basada en paquetes) 27

2.2.2.2 Subcapa de parte común 27

2.2.2.3 Subcapa de Seguridad 28

2.2.3 Capa física 28

2.2.3.1 Evolución 28

2.2.3.2 OFDM (Orthogonal Frecuency Division Multiplexing) 29

2.2.3.3 Tipos de modulación soportados por el estándar de WiMAX. 34

2.2.3.4 Topologías 35

2.2.3.5 Propagación NLOS y LOS 36

2.3 802.1Q VLAN **37**

2.3.1 Etiquetado de trama 802.1Q 37

2.3.1.1 Visión general del etiquetado de la trama de la VLAN 37

2.3.5 DTP 38

2.3.6 Modos de enlace troncal 38

2.3.7 Configurar un enlace troncal 802.1Q 40

2.4 Protocolos de VoIP **40**

2.4.1 Características VoIP 40

2.4.2 Protocolos de señalización 41

2.4.2.1 H.323 41

2.4.2.2 H.225 (Señalización de control de llamada) 42

2.4.2.3 H.245 (Control) 42
2.4.2.4 SIP (Session Initiation Protocol) 43
2.4.2.4.1 Mensajes SIP 44
2.4.3 Protocolos de Transporte 45
2.4.3.1 RTP (Real-Time Transport Protocol) 45
2.4.3.2 cRTP (Compress RTP) 46
2.4.4 Códecs 46
2.4.4.1 ITU G.711 47
2.4.4.2 ITU G.729 47
2.5 Estándares MPEG 47
2.6 FTP (File Transfer Protocol) 48
CAPÍTULO III 50
Equipo de red 50
3.1 BS WiMAX Redline 100AN-U 51
3.1.1 Características 51
3.1.2 Administración de las políticas de calidad 52
3.1.3 Parámetros de la interfaz aérea 57
3.1.4 Administración del equipo: 57
3.2 Estaciones Suscriptoras 59
3.2.1 SUI 59
3.2.2 SUO 60
3.2.3 Administración del equipo: 60
3.4 Switch CISCO serie Catalyst 2960 62
3.4.1 Switch 62
3.4.2 Características de los Switches Catalyst 2960 62
3.4.3 VLAN 62
3.4.4 Tipos de VLAN 63
3.4.4.1 VLAN de datos 63
3.4.4.2 VLAN nativa 63
3.4.4.3 VLAN de administración 63
3.4.4.4 VLAN de voz 64
3.4.5 Configuración de VLAN 64
3.4.6 Asignar un puerto de switch 64
3.4.7 Definición de enlace troncal de la VLAN 65
3.5 Router CISCO modelo 2811 65
3.5.1 Router 65
3.5.2 Caracteristicas del Router 2811 66
3.5.3 Rutas estáticas 66
3.5.3.1 El comando ip route 67

3.5.4 Subinterfaces 67
3.5.4.1 Configuración de la subinterfaz 68
3.5.5 Listas de Acceso 68
3.5.5.1 Características de las ACLs 69
3.5.5.2 Cómo funcionan las ACL 69
3.5.5.3 Tipos de ACLs 69
3.5.5.3.1 ACL estándar 69
3.5.5.3.2 ACL extendidas 70

3.6 TelefoníaVoIP 70
3.6.1 Configuración del Gatekeeper SPA9000 70
3.6.2 Configuración de los temporizadores 72
3.6.3 Parámetros RTP 72
3.6.4 Configuración de los teléfonos IP Linksys 73

CAPITULO IV 77

QoS y Aplicaciones de red 77

4.1 Calidad de servicio QoS 78
4.1.1 Ancho de banda disponible 78
4.1.2 Retraso de extremo a extremo 79
4.1.3 Variación del retraso 79
4.1.4 Pérdida de paquetes 80
4.1.5 Implementación de QoS 81
4.1.5.1 Identificación del tráfico y sus requerimientos 81
4.1.5.2 Definición de políticas para cada clase 81
4.1.6 Modelo de QoS 82
4.1.6.1 Modelo de servicios integrados 82
4.1.6.2 Modelo de servicios diferenciados 83
4.1.7 Implementación de QoS 84
4.1.7.1 (Differentiated Service Code Point) (DSCP) 85
4.1.7.2 Assured Forwarding 87
4.1.7.3 Expedited Forwarding 88

4.2 VLC Media Player 89

4.3 VSFTPD 94

4.4 iPERF 94

4.5 nTop 95

CAPITULO V 97

Red 97

5.1 Estructura 98

5.2 Configuración 99
5.2.1 Sin QoS 101
5.2.1.1 Configuración del Router conectado a la BS 102
5.2.1.2 Configuración del Router conectado al Subscriptor 103
5.2.1.3 Configuración del Switch conectado a la BS 104
5.2.1.4 Configuración del Switch conectado al Subscriptor 105
5.2.1.5 Configuración de flujos en la BS 106
5.2.2 Con QoS en el equipo CISCO 106
5.2.2.1 Configuración del Router conectado a la BS 106
5.2.2.2 Configuración del Router conectado al Subscriptor 108
5.2.2.3 Configuración del Switch conectado a la BS 108
5.2.2.4 Configuración del Switch conectado al Subscriptor 108
5.2.3 Con QoS de extremo a extremo 108

CAPITULO VI 109

Resultados 109

6.1 Sin QoS 110
6.1.1 Velocidad de transmisión máxima del canal de bajada (de extremo a extremo): 111
6.1.2 Análisis 1 Retardo en el canal de voz sin trafico en los demas segmentos 111
6.1.3 Análisis 2. Retardo en el canal de voz inyectando tráfico en el canal de datos mediante el software IPER 115
6.1.4 Análisis 3. Retardo en el canal de voz inyectando tráfico en el canal de datos mediante el software IPER e inyectando tráfico en el canal de video, mediante la descarga de un video 118
6.1.5 Análisis 4. Retardo en el canal de voz inyectando tráfico en el canal de datos mediante el software IPER he inyectando tráfico en el canal de video, mediante la descarga de 2 videos 122
6.1.6 Análisis 5. Retardo en el canal de voz inyectando tráfico en el canal de datos mediante el software IPERF e inyectando tráfico en el canal de video, mediante la descarga de 3 videos 126
6.1.7 Análisis 6. Retardo en el canal de voz inyectando tráfico en el canal de datos mediante el software IPER e inyectando tráfico en el canal de video, mediante la descarga de 4 videos 130
6.1.8 Análisis 7. Retardo en el canal de voz inyectando tráfico en el canal de video, mediante la descarga de 5 videos 134

6.2 Con QoS en el equipo CISCO 135
6.2.1 Análisis 1. Retardo en el canal de voz inyectando tráfico en el canal de datos mediante el software IPERF e inyectando tráfico en el canal de video, mediante la descarga de 4 videos 136

6.3 Con QoS de extremo a extremo. 138
6.3.1 Análisis 1. Retardo en el canal de voz 141

CAPITULO VII 144

Conclusiones 144

ÍNDICE DE FIGURAS:

Figura 1 Comparación del modelo OSI y el modelo TCP/IP……..20

Figura 2 Subcapas del protocolo 802.16-2004……27

Figura 3 Atenuación de las ondas radioeléctricas debido a la presencia de oxígeno y de vapor de agua……..30

Figura 4 Señal distorsionada por ISI (en el dominio del tiempo)……..31

Figura 5 Ejemplo de ICI……..32

Figura 6 Diagrama a bloques del modulador OFDM……..33

Figura 7 Par de transformadas discretas: Convolución circular – Producto……..34

Figura 8 Campo de etiqueta de la VLAN……38

Figura 9 Encabezados de protocolos RTP, UDP e IP……..45

Figura 10 RTP a cRTP……..46

Figura 11 BS WiMAX……51

Figura 12 Menú de SC……..54

Figura 13 Menú de SFs……55

Figura 14 Menú de clasificadores……..56

Figura 15 Menú de suscriptores……..58

Figura 16 Menú de configuración avanzada……59

Figura 17 SUI……..60

Figura 18 Ejemplo de aplicación de VLANs……..63

Figura 19 Ejemplo de una ruta estática……67

Figura 20 Pantalla inicial del SPA900……71

Figura 21 Configuración de la dirección WAN……71

Figura 22 Configuración de los temporizadores SIP y parámetros RTP……73

Figura 23 Configuración del teléfono IP Linksys……74

Figura 24 Configuración de los temporizadores SIP y de los parámetros RTP……75

Figura 25 Configuración del nombre del dispositivo……75

Figura 26 Configuración del número de extensión……76

Figura 27 Interfaz gráfica de VLC……89

Figura 28 Menú "Convertir"……90

Figura 29 Menú principal de emisión……90

Figura 30 Menú "Protocolo de envío"……91

Figura 31 Menú "Destinos"……92

Figura 32 Opciones de red……93

Figura 33 Reproducción de video en el cliente……93

Figura 34 Topología implementada……98

Figura 35 SC creadas en la BS ……100

Figura 36 Clasificadores creados en la BS……112

Figura 41 Respuesta ICMP del Router (tamaño paquete ICMP 1000)……112

Figura 42 Respuesta ping de PC de voz……113

Figura 43 Gráfica de los retardos de los paquetes ping……114

Figura 44 Respuesta ICMP del Router (ping repetido 1000)……115

Figura 45 Respuesta ICMP del Router (tamaño paquete ICMP 1000)……115

Figura 46 Respuesta ping de PC de voz……116

Figura 47 Gráfica de los retardos de los paquetes ping……117

Figura 48 Respuesta ICMP del Router (ping repetido 1000)……118

Figura 49 Respuesta ICMP del Router (tamaño paquete ICMP 1000)……118

Figura 50 Respuesta ping de PC de voz……119

Figura 51 Gráfica de los retardos de los paquetes ping……120

Figura 52 Imagen de un video transmitiéndose……121

Figura 53 Tasa de transmisión para un video……121

Figura 54 Respuesta ICMP del Router (ping repetido 1000)……122

Figura 55 Respuesta ICMP del Router (tamaño paquete ICMP 1000)……122

Figura 56 Respuesta ping de PC de voz……123

Figura 57 Gráfica de los retardos de los paquetes ping……124

Figura 58 Imagen de dos videos transmitiéndose……125

Figura 59 Tasa de transmisión para dos videos……125

Figura 60 Respuesta ICMP del Router (ping repetido 1000)……126

Figura 61 Respuesta ICMP del Router (tamaño paquete ICMP 1000)……126

Figura 62 Respuesta ping de PC de voz……127

Figura 63 Gráfica de los retardos de los paquetes ping……128

Figura 64 Imagen de tres videos transmitiéndose……129

Figura 65 Tasa de transmisión para tres videos……129

Figura 66 Respuesta ICMP del Router (ping repetido 1000)……130

Figura 67 Respuesta ICMP del Router (tamaño paquete ICMP 1000)……130

Figura 68 Respuesta ping de PC de voz……131

Figura 69 Gráfica de los retardos de los paquetes ping……132

Figura 70 Imagen de cuatro videos transmitiéndose……133

Figura 71 Tasa de transmisión para cuatro videos……133

Figura 72 Falló del programa Iperf……134

Figura 73 Imagen de cinco videos transmitiéndose……134

Figura 74 Tasa de transmisión para cinco videos……135

Figura 75 Respuesta ICMP del Router (ping repetido 1000)……136

Figura 76 Respuesta ICMP del Router (tamaño paquete ICMP 1000)……136

Figura 77 Respuesta ping de PC de voz……137

Figura 78 Tasa de transmisión para cuatro videos, con QoS CISCO……137

Figura 79 Imagen de un video transmitiéndose con QoS de extremo a extremo……138

Figura 80 Imagen de dos videos transmitiéndose con QoS de extremo a extremo……139

Figura 81 Imagen de tres video transmitiéndose con QoS de extremo a extremo……140

Figura 82 Tasa de transmisión para tres videos con QoS de extremo a extremo……..140

Figura 83 Respuesta ICMP del Router (ping repetido 1000)……141

Figura 84 Respuesta ICMP del Router (tamaño paquete ICMP 1000)……141

Figura 85 Respuesta ping de PC de voz……142

Figura 86 Resultados obtenidos en el cliente ftp……143

ÍNDICE DE TABLAS:

Tabla 1 Evolución del estándar 802.16……25

Tabla 2 Protocolos contenidos dentro de H.323……42

Tabla 3 Plantillas de WiMAX……57

Tabla 4 Configuración de una VLAN……64

Tabla 5 Configuración de un puerto de acceso en un Switch Tabla 6 Configuración de un puerto troncal en un Switch……65

Tabla 6 Configuración de un puerto troncal en un Switch……65

Tabla 7 Comparación de la interfaz del router y las subinterfaces……68

Tabla 8 Valores predeterminados de los temporizadores del protocolo SIP……72

Tabla 9 Valores predeterminados de los parámetros RTP……72

Tabla 10 Políticas de QoS……82

Tabla 11 Niveles de prioridad……87

Tabla 12 Valores de DSCP asociados a cada clase……88

Tabla 13 Valores estandarizados para DSCP…… 88

Tabla 14 Banderas del comando iPERF……95

Tabla 15 Direccionamiento IP de los dispositivos……99

Tabla 16 Características de las SC programadas……100

CAPÍTULO I

Antecedentes

1.1 Introducción

En la actualidad una gran cantidad de empresas utilizan redes de computadoras para la administración de sus recursos y/o actividades, dichas redes deben abarcar áreas geográficas de dimensiones considerables. La arquitectura con la que se implementa dicha red puede entenderse como una especie de islas denominadas LAN[1] (Local Area Network) conectadas a través de puentes (enlaces WAN), el conjunto de islas conectadas se denomina WAN (Wide Area Network). [1]

Los usuarios domésticos usamos la red que soporta el INTERNET como enlace WAN debido a su bajo costo, por lo mismo esta se encuentra constantemente ocupada por las transmisiones de muchos usuarios lo que dificulta la transmisión de determinados tipos de información como son la voz (telefonía) y la información multimedia (videos), además la información corre el riesgo de ser interceptada por terceros. Para fines de una empresa lo anterior no

[1]En la sección de Glosario se encuentra la definición de los acrónimos utilizados

es aceptable, cómo alternativa se implementa un enlace WAN privado, que ofrece un canal de comunicación exclusivo para los usuarios pertenecientes a la misma.

Existen diferentes tecnologías para implementar los enlaces WAN, por ejemplo: HDLC, PPP, Frame Relay; Sin embargo estas opciones requieren de medios guiados para su implementación (par trenzado, cable coaxial, fibra óptica) lo cual es un problema en caso de no existir infraestructura que cubra dicha área geográfica ya que se debe esperar hasta que sea creada, y el costo es elevado.

Las tecnologías de redes inalámbricas de banda ancha, denominadas BWA (Broadband Wireless Access), como indica su nombre se implementan "sin cables". De las tecnologías BWA existentes WiMAX representa una buena opción para la implementación del enlace WAN debido a que ofrece completa compatibilidad con el protocolo TCP/IP y puede basar la calidad de servicio basada en el encabezado del paquete IP.

1.2 Breve historia del desarrollo de las redes de computadoras.

El desarrollo de las redes de computadoras inició a finales de los años sesenta (1969), cuando el Departamento Americano de Defensa (DoD) observó que la Red Telefónica Conmutada presentaba el riesgo de quedar inutilizable si eran atacados ciertos nodos de su infraestructura.

El sistema diseñado para conservar la comunicación entre puntos estratégicos se denominó ARPAnet, el cual podía conseguir que la información llegara a su destino sin importar que parte de la red estuviera destruida. La característica que le permitió lograr tal resultado fue segmentar la información en paquetes, añadiendo a cada paquete un encabezado con información de su origen, destino, corrección de errores, etc. De esta manera el paquete no viajaba por una ruta preestablecida a través de la red, en vez de ello cada nodo se encargaba de encaminar el flujo de paquetes basado en la cabecera de cada paquete, de esta manera si parte de la red era destruida el flujo de paquetes era encaminado hacia una ruta alternativa.

En un inicio ARPAnet fue de uso exclusivo militar y académico, más adelante ARPAnet fue dividido en un versión de uso público y se mantuvo una versión exclusiva para el ejército. A su vez los desarrollos tecnológicos permitieron que particulares implementaran sus propias redes, para garantizar la interconectividad entre equipos creados por diferentes fabricantes en 1974 fue presentado el protocolo TCP/IP (basado en el modelo del mismo nombre). TCP/IP fue adoptado por ARPAnet hacia los ochenta. De la interconexión de

pequeñas redes de dominio particular y la versión pública de ARPAnet, ambos operando bajo TCP/IP, surgió INTERNET. [2]

Hace aproximadamente una década, el modo de acceso más común a nivel mundial era el módem. Dispositivo que, utilizando la infraestructura telefónica existente, permitía convertir las señales digitales de la computadora en señales analógicas que viajaban a través del tendido de cables (originalmente diseñados para enviar voz solamente) hacia la central de conmutación. A pesar de que esta tecnología denominada "dial-up", era conveniente, económicamente hablando, su rendimiento era limitado. Además, la necesidad de establecer una llamada telefónica para lograr dicho acceso, no era algo que muchos usuarios consintieran. Por esta razón, el acceso de banda ancha se desarrolló, permitiendo a los usuarios enviar texto, imágenes, sonidos y video a velocidades considerablemente mayores.

Ahora existen una variedad de técnicas para proporcionar a un nodo el acceso de banda ancha. De manera sencilla, se puede mencionar las siguientes:

La primera, es la tecnología híbrida de fibra óptica y cable coaxial utilizada por las compañías de TV por cable que aprovechan su infraestructura ya desplegada. En segundo lugar, se encuentra la tecnología más común en nuestros días: ADSL, cuyo funcionamiento se basa en la transmisión de señales de información a través del cableado telefónico a frecuencias más altas que las de la voz, utilizando un filtro en el extremo del usuario. A pesar de la publicidad y el marketing que se desarrollan entorno a estas tecnologías, los usuarios finales frecuentemente se encuentran ante los problemas de una velocidad de transmisión menor a la prometida e incluso un desempeño pobre. A continuación, el acceso por fibra óptica puede ser una buena opción si lo que se desea son altas velocidades, mediante las diferentes modalidades, siendo quizás la más común la Fibra a casa (Fiber-to-home). La desventaja actual de esta tecnología consiste en el costo de instalación y altos cuidados necesarios durante la instalación, el mantenimiento y la conservación de la conexión. Además de estas tecnologías alámbricas, actualmente se ha mostrado un fuerte interés en las tecnologías inalámbricas para resolver el problema del acceso de última milla. Así, la cuarta tecnología que permite el acceso de banda ancha es utilizar redes satelitales orientadas al acceso a Internet, similar al sistema de telefonía satelital Iridium en el que el suscriptor establece una comunicación directa con el satélite mediante una antena parabólica. Y por último, la quinta tecnología: una red BWA, que es fija, baja en costo y extremadamente conveniente en aquellos lugares donde el despliegue de líneas telefónicas o fibra óptica no es rentable o no está planeado aún. Por ejemplo, en

lugares montañosos o de difícil acceso técnico, las tecnologías alámbricas no serán de ninguna manera la mejor opción para prestar el servicio de acceso de banda ancha.

1.3 Definición del problema

El estándar IEEE 802.16-2004 describe la tecnología WiMAX para enlaces entre terminales fijos, a su vez indica que dichos equipos deben ser capaces de ofrecer calidad de servicio sobre las transmisiones. Por ello se pueden transmitir voz, video y datos sobre dichos enlaces. Otra característica de WiMAX es que es una tecnología de bajo costo, por ello podría utilizarse como una alternativa al enlace WAN en caso de no disponer de infraestructura, además que dicho enlace sería convergente.

Por lo anterior es necesario contar con estudios experimentales para analizar el desempeño de los diversos servicios (voz, video y datos) en enlaces realizados por medio de equipos certificados.

1.4 Objetivos

Éste trabajo tiene como objetivo analizar el desempeño de los servicios ofrecidos en los extremos del enlace WAN, dicho enlace tendrá la capacidad de transmitir voz, video y datos sobre el protocolo IP. También se verifica la interoperabilidad, específicamente con equipos de red de la marca CISCO.

Al final los resultados servirán para comparar cómo la calidad de servicio (QoS) tanto del equipo WiMAX, cómo del equipo de red LAN afectan el desempeño de los servicios (voz, video y datos).

1.5 Método

Se realizarán pruebas con la intención de observar el comportamiento y las prestaciones de una red WiMAX, así como las diferentes calidades de servicio (QoS) implementadas para la transmisión multimedia a través de la red.

Para el estudio instrumental, se utilizarán 1 BS WiMAX, 1 usuarios subscriptores, 2 ruteadores CISCO, 2 switches y 1 laboratorio de VoIP.

1.5 Estructura de la tesis

El capítulo 1 describe cómo fue el desarrollo de las redes de datos con el fin de recalcar la importancia de la interoperabilidad entre equipos de diferentes fabricantes. También se enumeran las tecnologías actuales que ofrecen el acceso de banda ancha y las desventajas que presentan al emplear medios de transmisión guiados, se menciona el uso de redes BWA y sus ventajas para cubrir zonas de difícil acceso. Finalmente se exponen las características de la tecnología WiMAX que la convierten en una buena opción como red BWA convergente.

El capítulo 2 se compone de una descripción de los protocolos usados por el equipo de red y por las aplicaciones. Se comienza por explicar el modelo de referencia OSI y el modelo de red TCP/IP. Se describe la evolución del estándar WiMAX, y las especificaciones de la subcapa MAC y la capa física del estándar IEEE 802.16-2004 (WiMAX fijo). Se describen las funciones del protocolo 802.1Q VLAN para ayudar a la implementación del QoS en los extremos de la red. Y por último se enumeran las características de los protocolos usados para el procesamiento de la señal de voz y video G.XX, MPEG-XX.

El capítulo 3 comienza por la descripción de los componentes físicos de la BS WiMAX, su software y la administración de la misma. Se continúa por describir las unidades suscriptoras (SS) tanto de interior cómo de exterior, se mencionan características tanto de hardware cómo de software y su administración. Se prosigue por describir los componentes básicos y el mecanismo de operación de los equipos de red (switch y router). Finalmente se describen las aplicaciones usadas para implementar cada servicio (voz, video, datos).

El capítulo 4 es prácticamente un manual en el cuál reportamos todas las configuraciones tanto las hechas en los equipos de red, cómo las realizadas en las aplicaciones, incluyendo el direccionamiento.

El capítulo 5 es el reporte de la calidad de las transmisiones recibidas en función de los parámetros de QoS implementados en el la red y de la saturación del sistema.

El capítulo 6 son las conclusiones de las observaciones realizadas en el capítulo 5.

CAPÍTULO II

Estándares y protocolos empleados

Todo sistema de comunicaciones se compone de emisor, receptor, mensaje, canal, y reglas. La función de las reglas es coordinar a los demás componentes para que los mensajes puedan ser enviados y descifrados correctamente. En la práctica dichas reglas reciben el nombre de protocolos y son elaborados por organismos internacionales con el fin de establecer un marco común para que los equipos de distintos fabricantes sean interoperables.

En este capítulo se describen los protocolos empleados por los servicios de voz, video y datos, así como por el radioenlace WiMAX y los equipos de red CISCO.

2.1 Modelo OSI

El modelo OSI fue diseñado por la Organización Internacional para la Estandarización (ISO, International Organization for Standardization) para proporcionar un esquema sobre el cual crear una serie de protocolos. Cuyo objetivo era que este conjunto de protocolos se utilizara para desarrollar una red que no dependiera de sistemas propietarios.

El modelo OSI proporciona 7 capas, en las cuales se definen funciones específicas. También describe la interacción de cada capa con las capas directamente por encima y por debajo de estas.

Capas del modelo OSI:

- FISICA
- ENLACE DE DATOS
- RED
- TRANSPORTE
- SESIÓN
- PRESENTACIÓN
- APLICACIÓN

Por otro lado esta las suite de protocolos TCP/IP, estos protocolos pueden describirse en términos del modelo de referencia OSI.

Modelo TCP/IP

- APLICACIÓN
- TRANSPORTE
- INTERNET
- ACCESO A LA RED

Algunas similitudes entre el modelo TCP/IP y el modelo OSI, son las siguientes:

En la capa de acceso a la red, TCP/IP no especifica cuáles protocolos utilizar cuando se transmite por un medio físico; sólo describe la entrega desde la capa de Internet a los protocolos de red física. Las capas OSI 1 y 2 tratan los procedimientos necesarios para acceder a los medios y las maneras físicas de enviar datos por la red.

La semejanza clave entre TCP/IP y OSI se produce en la Capa 3 y 4 del modelo OSI. La Capa 3 del modelo OSI, se usa para describir todos los procesos que se producen en todas las

redes de datos para direccionar y enrutar mensajes a través de una internetwork. El Protocolo de Internet (IP) es el protocolo de la suite TCP/IP que incluye la funcionalidad descrita en la Capa 3.

La Capa 4, se utiliza para describir los servicios o funciones generales que administran las conversaciones individuales entre los hosts de origen y destino. Estas funciones incluyen ACK, recuperación de errores y secuenciamiento.

La capa de aplicación TCP/IP incluye un número de protocolos que proporciona funcionalidad específica a una variedad de aplicaciones de usuario final. Las Capas 5, 6 y 7 del modelo OSI se utilizan como referencias para proveedores y programadores de software de aplicación para fabricar productos que necesitan acceder a las redes para establecer comunicaciones.

La siguiente figura muestra la comparación entre el modelo OSI y el modelo TCP/IP.

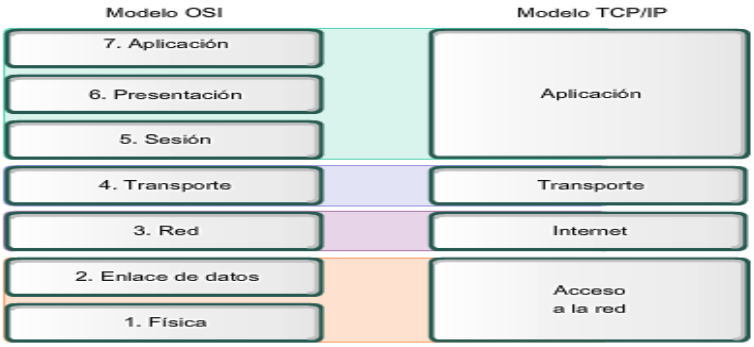


Figura1 Comparación del modelo OSI y el modelo TCP/IP [3]

2.1.2 Breve explicación de las capas del modelo OSI

Capa de Aplicación

La capa de aplicación, es la capa superior de los modelos OSI y TCP/IP. Es la capa que proporciona la interfaz entre las aplicaciones que utilizamos para comunicarnos y la red en la cual se transmiten los mensajes. Los protocolos de capa de aplicación se utilizan para intercambiar los datos entre los programas que se ejecutan en los hosts de origen y destino.

La capa de presentación

La capa de presentación tiene tres funciones principales:

- Codificación y conversión de datos de la capa de aplicación para garantizar que los datos del dispositivo de origen se puedan interpretar por la aplicación adecuada en el dispositivo de destino.
- Compresión de los datos de forma que los pueda descomprimir el dispositivo de destino.
- Encriptación de los datos para la transmisión y la encriptación de los mismos cuando lleguen a su destino.

La capa de sesión

Las funciones en esta capa crean y mantienen diálogos entre las aplicaciones de origen y destino. La capa de sesión maneja el intercambio de información para iniciar los diálogos y mantenerlos activos, y para reiniciar sesiones que se interrumpieron o desactivaron durante un periodo de tiempo prolongado.

La capa de transporte

La capa de transporte permite la segmentación de datos y brinda el control necesario para reensamblar las partes dentro de los distintos segmentos de comunicación. Las responsabilidades principales que debe cumplir son:

- Rastreo de comunicación individual entre aplicaciones en los hosts de origen y destino
- Segmentación de datos y manejo de cada parte
- Reensamble de segmentos en streams de datos de aplicación
- Identificación de diferentes aplicaciones

La capa de red

Provee servicios para intercambiar datos individuales a través de la red entre dispositivos finales. Para realizar este transporte de extremo a extremo la Capa 3 utiliza cuatro procesos básicos:

- Direccionamiento
- Encapsulación
- Enrutamiento

- Desencapsulación

La capa de enlace de datos

Proporciona un medio para intercambiar datos a través de medios locales.

La capa de enlace de datos realiza dos servicios básicos:

- Permite a las capas superiores acceder a los medios usando tramas.
- Controla cómo se ubican los datos en los medios y cómo se reciben desde los medios usando técnicas como el control de acceso a los medios y la detección de errores.

La capa física

Proporciona los medios de transporte para los bits que conforman la trama de la capa de Enlace de datos a través de los medios de red. Esta capa acepta una trama completa desde la capa de Enlace de datos y la codifica como una secuencia de señales que se transmiten en los medios locales.

El envío de tramas a través de medios locales requiere los siguientes elementos de la capa física:

- Medios físicos y conectores asociados
- Una representación de los bits en los medios
- Codificación de los datos y de la información de control
- Sistema de circuitos del receptor y transmisor en los dispositivos de red

2.2 Estándar 802.16-2004, tecnologías WiMAX

Al estar definido por un estándar la gran ventaja de un equipo WiMAX, es la interoperabilidad que significa que este puede comunicarse con cualquier otra tecnología basada en estándares IEEE.

WiMAX (versión fija) es una certificación que reciben equipos BWA que cumplen con determinadas funciones y características establecidas por el estándar 802.16-2004; Sin embargo el protocolo se ha modificado varias veces, creándose así diversas versiones del estándar desde su creación, algunas añaden funciones o mejoran las existentes, otras son recopilaciones o correcciones.

En la actualidad la versión oficial es la IEEE 802.16-2009 que es la revisión y agrupación (consolidación) de los estándares 802.16-2004 (802.16-2001, 802.16c-2003, 802.16a-2002), 802.16e-2005 y 802.16-2004/Cor1-2005, 802.16f-2005 y 802.16g-2007. [4]

2.2.1 Evolución del estándar IEEE 802.16-2009

El Instituto de Ingenieros en Electricidad y Electrónica (IEEE) surgió como la fusión de sus dos predecesores: el Instituto Norteamericano de Ingenieros Eléctricos (AIEE) y el Instituto de Ingenieros en Radio (IRE) por medio de un plan que entró en vigor el 1o. de enero de 1963. Actualmente, el IEEE es la organización técnica y profesional más grande y prestigiada del mundo. De acuerdo a lo publicado en su sitio de internet, tienen como objetivos científicos/educativos promover el avance de las teorías y las prácticas de la electrotecnologia; en el ámbito profesional, fomentar el progreso y el desarrollo profesional de su membresıa y en el terreno social, mejorar la calidad de vida a través de la aplicación de la electrotecnologıa, así como promover el entendimiento de la electrotecnologıa ante el público.[2]

El grupo de trabajo IEEE 802.16 sobre Estándares de Acceso Inalámbrico de Banda Ancha(Broadband Wireless Access Standards)fue creado en 1999 y tiene como función principal desarrollar estándares y prácticas recomendadas que apoyen el despliegue de las Redes Inalámbricas de Área Metropolitana (WMAN). Este grupo es una unidad perteneciente al Comité de Estándares IEEE 802 LAN/MAN y se encuentra dividido a su vez en dos grupos de trabajo: 802.16 y 802.16a.

El grupo de trabajo 802.16 creó los estándares 802.16-2001 y 802.16c-2002. Mientras que el El grupo de trabajo 802.16a creó el estándar 802.16a-2003. Finalmente el estándar 802.16-2004.fue la revisión y consolidación de estos.

En general el 802.16-2001 aporta las técnicas para trabajar con línea de vista (LOS), mientras que el 802.16a-2003 las referentes para hacerlo sin ella (NLOS). La principal diferencia entre estos estándares es la banda de frecuencias de operación, para el grupo de trabajo 802.16 era de 10-66 [GHz] mientras que para el grupo 802.16 a era de 2-11 [Ghz], siendo esta última la que se adoptó para el 802.16-2004.

A partir del estándar 802.16e-2005 se comenzaron a emitir diversas versiones del 802.16 para versión móvil de WiMAX (802.16-2004/Cor1-2005, 802.16f-2005, 802.16g-2007) hasta llegar a la revisión y consolidación de estas más la del 802.16-2004 que es el estándar 802.16-2009 anteriormente nombrado.

Diferentes escenarios para la prestación del servicio de WiMAX deben ser considerados. Cada uno de ellos cuenta con conceptos distintos que deben ser bien diferenciados:

El acceso fijo de banda ancha provisto por WiMAX es una aplicación en la cual tanto la BS como la SS se encuentran fijas en una posición durante la operación. Este tipo de acceso es común en entornos residenciales, en donde es sencillo fijar la SS, ya sea al interior o al exterior del edificio, con el fin de transmitir hacia la BS. Al no encontrarse en movimiento, esta modalidad permite alcanzar mayores velocidades de transmisión. Con ello, aplicaciones como Internet, TV por IP y Video Bajo Demanda (VoD) son ahora posibles sin la necesidad de utilizar la fibra óptica o el sistema de cable actual.

El acceso móvil de Banda Ancha hace referencia a la capacidad de un usuario de estar en movimiento, al mismo tiempo que una operación se esté llevando a cabo o no. En la mayoría de los casos, la BS nunca cambia de posición y es la SS la que se considera móvil, recibiendo entonces el nombre de estación móvil (MS).

Así mismo, existen tres términos que en la vida cotidiana presentan confusión pero que deberían utilizarse correctamente: nomadicidad, movilidad y portabilidad. Imaginemos un escenario en el que dos estaciones base contiguas pertenecen al mismo operador. Un usuario que realiza un hand-off entre una y otra deberá iniciar una sesión nuevamente. A esto se le llama nomadicidad.

Ahora, el concepto de movilidad ocurre cuando el usuario puede viajar a lo largo de varias celdas cubiertas por diferentes estaciones base sin la interrupción de su transmisión de datos, voz o video y sin un límite de velocidad que condicione este movimiento. Y, por último, el concepto de portabilidad se presenta cuando el usuario puede moverse a una velocidad razonablemente alta (alrededor de los 120 km/hr) sin la interrupción de una posible sesión o una comunicación abierta.

La siguiente tabla resume las características de las versiones del 802.16 que se han publicado a la fecha:

Versión	Descripción
802.16	Publicado en abril 2002, es el primer conjunto de especificaciones, contiene las referentes para operar en el intervalode frecuencias de 19 a 66 GHz exclusivamente con línea de vista y en topología PTMP. La máxima velocidad de transmisión es de 134 Mbps en celdas de hasta 5 km.
802.16 a	Publicado en enero de 2003, es una expansión del 802.16 para operar en el intervalo de frecuencias de 2 a 11 GHz, soportar transmisiones LOS y NLOS, así como topologías PTP, PTMP
802.16 c	Publicado en abril de 2003, es una expansión del 802.16 para especificar las operaciones en el intervalo de frecuencias de 10 a 66 GHz
802.16 d	Publicado oficialmente como la versión 802.16-2004. Agrupa la revisión de las versiones anteriores más los perfiles aprobados por WiMAX fórum.
802.16 e	Publicado en diciembre de 2005, extensión de la versión anterior que incluye las especificaciones para los dispositivos móviles.

Tabla 1 Evolución del estándar 802.16 [4]

2.2.2 Subcapa MAC

Los dispositivos basados en el estándar 802.16-2004 cumplen con una arquitectura de red basada en la subdivisión en capas de acuerdo al modelo de interconexión para sistemas abiertos (OSI), y especifican determinadas características de la subcapa MAC (dentro de la capa de enlace de datos) y la capa física.

Desde la publicación de los estándares IEEE 802.x se dividió la capa de enlace da datos en las subcapas LLC y MAC con la finalidad de tener una interfaz compatible con el protocolo de la capa de red sin importar el medio físico utilizado para la transmisión. [3]

Para explicar cómo se maneja el paquete una vez que es transferido hacia dichas capas es necesario describir los siguientes términos debido a que cuándo un la información se desplaza a través de la torre de protocolos recibe una denominación determinada, estos términos son:

- SDU(Service Data Unit): Se denomina así a la unidad de datos cuando asciende o desciende en la torre de protocolos, dichos protocolos deben ser adyacentes.
- PDU(Protocol Data Unit): Es la unidad de datos intercambiada entre protocolos en la misma altura de la torre de protocolos pero en puntos (ubicaciones) distintos.

Además es conveniente mencionar que son las siguientes definiciones y variables:

- SAP(Service Acces Point): Punto en la torre de protocolos donde los servicios de una capa inferior están a disposición para la capa adyacente superior a esta.
- SFID(Service-Flow Identifier): Identificador de SF, es un valor de 32 bits.
- CID(Connection Identifier): Es un valor de 16 bits que identifica una conexión unidireccional entre la BS y una SS, a su vez se asocia a un service-flow mediante el apeo con un SFID. En la sección de descripción del equipo se hará un descripción más amplia acerca de la implementación de dichas conexiones,y de los servicios de flujo (service-flow).

En general la subcapa MAC del estándar 802.16-2004 cumple las funciones de:

1. Convertir la SDU recibida de la subcapa LLC a una MAC PDU.
2. Seleccionar el flujo al que corresponde la PDU por medio del CID y del SFID asociado.
3. Brindar calidad de servicio (QoS) a través del mapeo del SFID a determinada “clase de servicio”, este concepto comprende los mecanismos de “schedulling”, todo esto se desarrolla a detalle en el capítulo de descripción del equipo.
4. Administrar retransmisiones de PDU’s de ser requeridas.
5. Proporcionar seguridad sobre el canal inalámbrico.

El estándar 802.16-2004 a su vez subdivide la subcapa MAC en tres porciones:

1. Subcapa de convergencia para servicios específicos (ATM o basada en paquetes).
2. Subcapa de parte común.
3. Subcapa de privacidad.

La figura siguiente representa la pila de subcapas que describe el estándar 802.16-2004

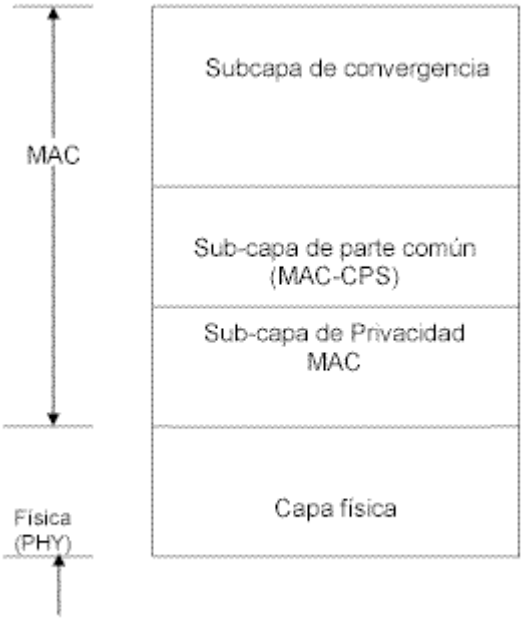


Figura 2 Subcapas del protocolo 802.16-2004 [4]

2.2.2.1 Subcapa de convergencia para servicios específicos CS (ATM o basada en paquetes)

Las especificaciones se inclinan por el uso del protocolo IP para la administración de las MAC PDU's, para ello la subcapa de convergencia realiza un mapeo entre las direcciones IP de los dispositivos que conforman la red y las direcciones de las conexiones MAC (CID).

La Subcapade convergencia también cuenta con la capacidad de supresión de cabecera (SPH Supression Protocol Header), esto es suprimir el encabezado de la capa superior, esto resulta útil al momento de enviar la información a través de la interfaz aérea debido a que las direcciones IP origen y destino se encuentran "atadas" a la dirección MAC por medio de dicho mapeo (CID). Al no transmitir los datos de la cabecera se consigue ahorrar ancho de banda del canal. [4]

2.2.2.2 Subcapa de parte común

Esta subcapa es independiente del protocolo de capa superior, realiza sus acciones basado en el CID. Es responsable de administrar el acceso al medio y con ello las políticas de calidad de servicio (QoS). [4]

En el estándar 802.16-2004 la calidad de servicio se asigna por medio de "plantillas", la plantilla tiene como parámetros determinados valores de campos de la cabecera del

paquete IP y un tipo de "schedulling", esto es un tipo de tráfico determinado. Si los valores del paquete que está siendo procesado coinciden con la plantilla el paquete se envía a la interfaz aérea respetando las características del tipo de "schedulling" indicado en dicha plantilla. La definición de "schedulling", los tipos de esté, los campos del encabezado IP así como el proceso para realizar la plantilla se describen más a detalle en el capítulo III Equipo de red y aplicaciones.

La retransmisión de información suele dejarse en responsabilidad de protocolos de las capas superiores; Sin embargo el estándar 802.16-2004 define mecanismos para que esta subcapa gestione la retransmisión de tramas.

2.2.2.3 Subcapa de Seguridad

Se consideran principalmente dos tipos de amenazas, la primera la violación de privacidad, esto es que alguien logré acceder y utilizar la información de un usuario válido sin su consentimiento, la segunda es el acceso no autorizado a los servicios, esto es que alguien sea capaz de usar los servicios sin autorización del administrador del equipo.

La privacidad se protege a través del cifrado de la comunicación entre la BS y cada SS (AES, 3DES). La llave de encriptación es distribuida sólo por la BS hacia las estaciones suscriptoras registradas (PKMv2), además se emplean certificados digitales X.509 para garantizar la identidad de las estaciones, de esta manera también se controla el acceso a la red, puesto que sólo las estaciones suscriptoras dadas de alta por el administrador en la BS reciben una llave. [4]

2.2.3 Capa física

2.2.3.1 Evolución

La parte del protocolo 802.16-2004 que corresponde a la capa física (PHY) es la responsable de establecer la conexión a través del medio físico entre los extremos de la conexión.

En general define las características de la interfaz de radio que va a utilizarse. Por ejemplo: el rango de la potencia de la señal, la técnica de modulación y demodulación, el acceso al múltiple, codificación, incluso las características que deben cumplir las antenas tanto de la BS como de las estaciones suscriptoras.

El estándar WiMAX trabaja bajo la técnica de modulación OFDM; Sin embargo enumera cuatro tipos diferentes de interfaces de radio, esto se debe a la propia evolución del estándar. Las principales diferencias son la banda de frecuencia en que operan, y el soporte

de transmisión sin línea de vista (NLOS) que se debe al tipo de modulación utilizada. Estas variantes son:

Red de Área Metropolitana Inalámbrica con una Sola Portadora (WMAN- SC, Wireless Metropolitan Area Network – Simple Carrier)

Red de Área Metropolitana Inalámbrica con Acceso a una Sola Portadora (WMAN-SCa, Wireless Metropolitan Area Network - Single Carrier access)

Red de Área Metropolitana Inalámbrica con Multiplexaje por División de Frecuencias Ortogonales (WMAN-OFDM Orthogonal Frequency Division Multiplexing)

Red de Área Metropolitana Inalámbrica con Múltiple Acceso por División de Frecuencia Ortogonal (WMAN-OFDMA, Orthogonal Frequency Division Multiple Access)

WMAN-SC es la primera versión, esta se diseñó para operar en el rango de frecuencias de 10 a 66 [GHz], no soporta trasmisiones sin línea de vista. WMAN-SCA es la mejora de la primera versión, esta sí soporta la trasmisión NLOS y opera en la banda de frecuencia debajo de 2 a 11 [GHz]; Sin embargo aún utilizaba la tecnología de una portadora (SC) por lo que no se alcanzaban altas tasas de transmisión. Con WMAN-OFDM se modificó la modulación, la técnica empleada fue OFDM, dicha técnica se describe a detalle a continuación; Sin embargo puede mencionarse que se divide el canal de radio en varios subcanales los cuales poseen las características de: transmitirse sin agregar bandas de guarda entre los subcanales, resistencia al ISI (interferencia entre símbolo), y la respuesta del canal se considera plana en cada subcanal. Esta modificación se definió en el estándar del año 2004 (WiMAX fijo), se fijó el número de subcanales en 254 (número de portadoras). Finalmente la última capacidad que se ha agregado en la especificación WMAN-OFDMA es la asignación de un grupo de subcanales a un usuario determinado y se incrementó el número máximo de portadoras a 2048; Sin embargo un número mayor a 254 portadoras se implementa para la versión móvil.[5]

2.2.3.2 OFDM (Orthogonal Frecuency Division Multiplexing)

OFDM es una técnica de multiplexaje (y modulación) multiportadora. Puede verse cómo una adaptación de la modulación en frecuencia que es capaz de transmitir en banda ancha y alcanza altas velocidades de transmisión.

Sistemas monoportadora (SC)

La principal limitante del ancho de banda en los sistemas que ocupan una sola portadora es la atenuación selectiva en frecuencia. Esto es que determinadas componentes del espectro de la señal son atenuadas, puede deberse a la interferencia de la señal con sigo misma después de descomponerse y viajar por multitrayectorías, o incluso a la atenuación propia del aire (puede observarse el comportamiento de la atenuación respecto a la frecuencia en la siguiente figura). Los sistemas de una sola portadora necesitan recibir todas las componentes del espectro de la señal para poder leer la información, por eso sus canales usan bandas de frecuencias pequeñas y ubicadas a manera de evitar la atenuación selectiva. Además se dejan porciones del espectro radioeléctrico sin utilizar entre los canales con el fin de evitar el traslape con el espectro de la señal de otro canal.

Un ejemplo de cómo afectan los fenómenos atmosféricos a las señales radioeléctricas se muestra en la siguiente figura, donde puede apreciarse la atenuación debida a la simple presencia del oxígeno y del vapor de agua:[6]

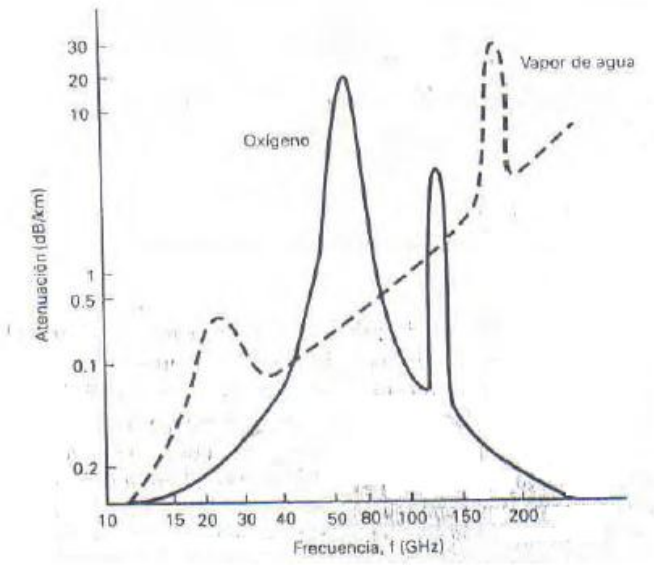


Figura 3 Atenuación de las ondas radioeléctricas debido a la presencia de oxígeno y de vapor de agua [6]

ISI (Inter Simbol Interference)

La tasa de transmisión es una medida de la cantidad de información capaz de enviarse a través del medio por unidad de tiempo, se mide en símbolos por segundo.

El canal inalámbrico presenta una limite en la tasa de transmisión debido principalmente a la interferencia entre símbolos, esta es el traslape de los símbolos (en el dominio del tiempo).

En sistemas NLOS la señal choca con obstáculos que generan la fragmentación de la señal original, y su desplazamiento a través de diferentes trayectorias. Los fragmentos de la señal original llegan a su destino con diferentes retardos, así el símbolo original se ve expandido en el tiempo pudiendo traslaparse con el siguiente símbolo en transmitirse.[5]

Se denomina τ como el retardo máximo introducido por el medio de propagación y Ts cómo la duración del símbolo. Si τ es comparable con Ts los símbolos quedan irreconocibles para el sistema, por otra parte en el caso de que Ts >>τ el sistema es aún capaz de extraer la información gracias a que la duración de la interferencia es despreciable.

En la parte superior de la siguiente ilustración se representan los fragmentos de la señal original que llegan al receptor, la parte inferior es la suma de dichos fragmentos, esta es la señal distorsionada por el ISI

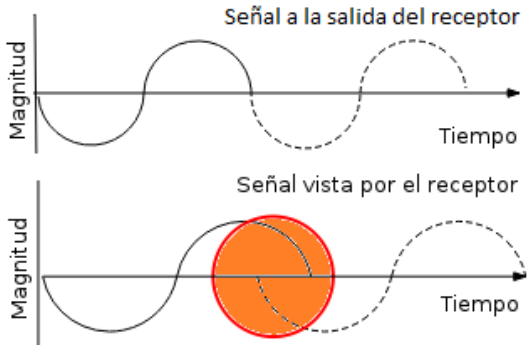


Figura 4 Señal distorsionada por ISI (en el dominio del tiempo)

ICI (Inter Carrier Interference)

Es el traslape del espectro de señales pertenecientes a distintos canales (en el dominio de la frecuencia). Sí al procesar la señal se introducen cambios bruscos en la señal el dominio del tiempo como truncamientos, ISI, o impulsos se generan componentes de alta frecuencia que expanden su espectro y pueden provocar el traslape con otro canal. [7]

La siguiente ilustración es una representación del espectro de dos señales, en el primer caso estas se consideran ortogonales porque en la componente de la portadora una señal alcanza su máximo valor de potencia mientras que la otra se mantiene en cero. Cuando esto deja de cumplir una canal interfiere con el otro, esto se denomina ICI.

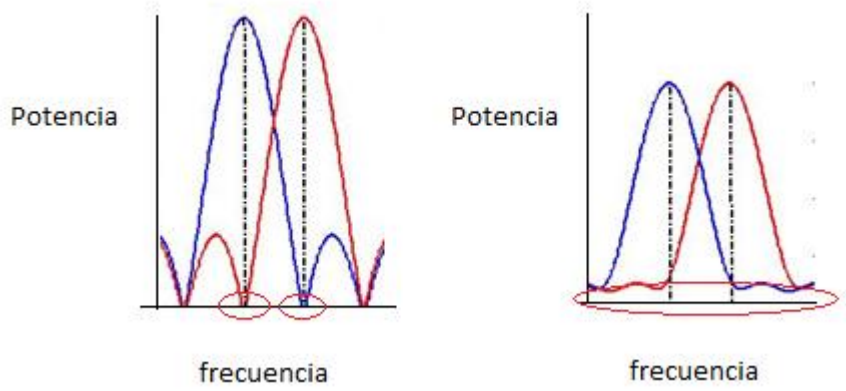


Figura 5 Ejemplo de ICI

La técnica OFDM es capaz de mitigar las atenuaciones selectivas, la ISI e ICI. Su funcionamiento es el siguiente:

1) Toma una alta tasa de transmisión y la divide en N flujos de una menor tasa de transmisión.

La primera etapa se implementa con un convertidor serial a paralelo, el cual divide el flujo principal a los N subcanales. Cada subcanal cuenta con un modulador 64QAM el cual reduce aún más la tasa de transmisión de cada subcanal.

Este paso incrementa la duración de Ts haciendo al sistema robusto contra la ISI. Además haciendo uso de diferentes subcanales si se presenta atenuación selectiva sólo algunos subcanales son afectados, los demás pueden transmitiendo sin problemas.

2) "Disfrazar" los símbolos de los subcanales como el espectro de una señal (la moduladora).

Se implementa a través de la IFFT (especificada de 254 puntos para WiMAX fijo), esta es una transformación del dominio de la frecuencia al dominio del tiempo.

La IFFT (FFT) presenta la ventaja de que el espectro se representa mediante componentes discretas, finitas y equiespaciadas. Al ser discretas y finitas pueden obtenerse a partir de los valores de los símbolos QAM en los subcanales. El separación entre las componentes puede manipularse, esta representa la banda de guarda y puede reducirse al mínimo. Además representados mediante diferentes frecuencias los canales son ortogonales entre sí. [4]

3) La salida de la IFFT es enviada a un convertidor paralelo-serial, anteriormente le es agregado el prefijo cíclico (Cyclic Prefix).

La secuencia a la salida del convertidor paralelo a serial es la base del símbolo OFDM. Con el fin de combatir la ISI e ICI parte del comienzo de secuencia es copiada y agregada al final de la secuencia original, dicha copia se denomina prefijo cíclico.

El prefijo cíclico tiene una duración que es usada como tiempo de guarda para contrarrestar el ISI. Si cómo tiempo de guardia se cesa la transmisión se genera un cambio brusco en la secuencia lo cual expande su espectro y genera ICI entre los subcanales, en cambio el prefijo cíclico sigue el mismo comportamiento de la secuencia original por lo que la modificación del espectro es mínimo o nula y se garantiza la ortogonalidad de los subcanales.

4) La secuencia más el prefijo son convertidos a una señal analógica la cual es modulada y radiada al aire. El proceso de recepción involucra los mismos bloques pero en sentido inverso.

El diagrama siguiente es el diagrama a bloques sobre el cuál se realiza el proceso descrito:

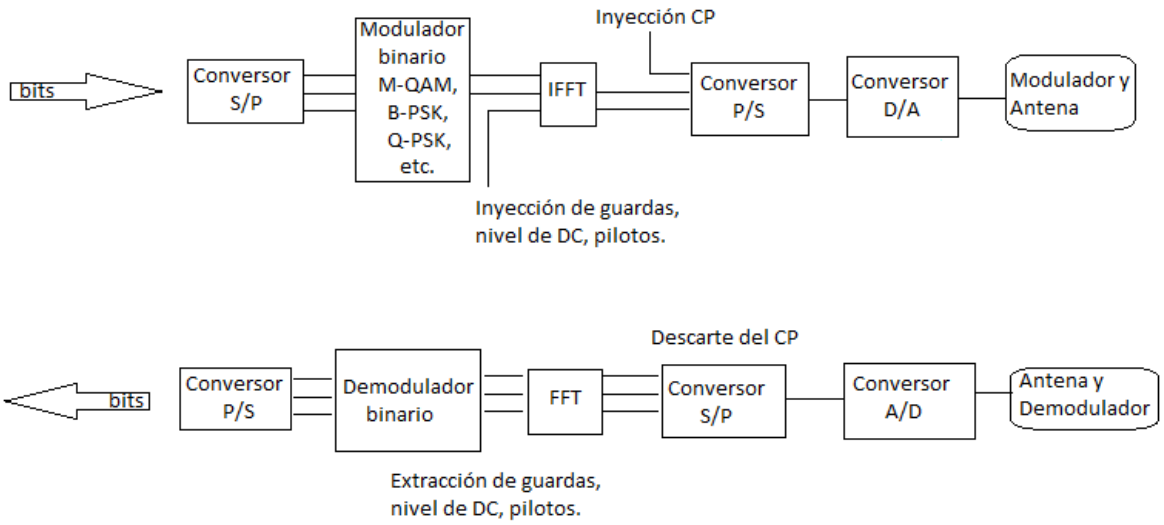


Figura 6 Diagrama a bloques del modulador OFDM [4]

También puede comprobarse la ortogonalidad mediante las propiedades matemáticas de la transformada rápida de Fourier de la convolución circular. [4]

Cuando la señal atraviesa el aire la secuencia sufre una convolución lineal con la respuesta al impulso del aire; Al agregar el prefijo cíclico la convolución genera una secuencia

periódica, los valores de un periodo de dicha secuencia son iguales a los obtenidos mediante la convolución circular de la secuencia original con la respuesta al impulso del aire. [4]

La transformada rápida de Fourier de la convolución circular consta en la multiplicación de la FFT de la secuencia del símbolo con la FFT de la respuesta al impulso del canal. Puede apreciarse que el resultado es el escalamiento del espectro de x[n] más no se agregan, o desplazan sus componentes por lo que se conserva la ortogonalidad.

Las funciones de convolución circular en el tiempo y de producto en el dominio de la frecuencia son:

$$y[n] \equiv f[n] \circledast h[n]$$
$$Y[k] = F[k]H[k]$$

Figura 7 Par de transformadas discretas: Convolución circular - Producto

2.2.3.3 Tipos de modulación soportados por el estándar de WiMAX.

Modulación BPSK (Binary Phase Shift Keying)

BPSK es una modulación digital binaria de fase. Esto es, que cada símbolo de la modulación está representado por un bit (por sus dos posibles valores: 0 y 1). El resultado de esta modulación es una señal muy robusta e inmune al ruido al elegir entre π y −π de acuerdo al valor del bit de información. Una de las formas más comunes de ilustrar una modulación digital es mediante el uso de la constelación, la cual se muestra a continuación para BPSK. [6]

Modulación QPSK (Quadrature Phase Shift Keying)

Cuando se desea tener mayor eficiencia espectral, es decir, tener más b/s por cada Hz (b/s/Hz) de ancho de banda, se recurre a modulaciones de mayor orden, justificando la elección de la modulación QPSK por encima de BPSK. [6]

Similar a la modulación BPSK, esta modulación consiste en dos bits para representar cuatro posibles fases con una separación de π/2 entre ellas. Por ejemplo: En el receptor, la demodulación es más complicada, pues es más difícil decidir entre que entre”0τ” “1”(como en BPSK). [6]

Es por ello que se dice que la modulación QPSK presenta menor inmunidad al ruido. Es importante recordar que mientras mayor sea la modulación, será más eficiente espectralmente, pero menos robusta ante el ruido. La siguiente figura ilustra la constelación para la modulación QPSK.

QAM (Quadrature Amplitude Modulation): 16-QAM y 64-QAM

La modulación QAM cambia las amplitudes de dos portadoras sinusoidales dependiendo de la secuencia que deba ser transmitida; las portadoras se encuentran desfasadas entre sí $+\pi/2$, esta modulación de amplitud es llamada cuadratura. De acuerdo a la teoría de comunicaciones digitales, gracias al concepto de cuadratura, la modulación 4-QAM resulta ser la misma que la modulación QPSK.

La modulación 64-QAM es la más eficiente (b/s/Hz) incluida en el estándar 802.16; en ella, se transmiten 6 bits por cada símbolo de la modulación. [6]

Modulación adaptable

El concepto de una modulación adaptable hace referencia a una técnica inteligente automatizada para mantener eficientemente un enlace de radio, incluso en condiciones adversas (atenuación, interferencias, obstáculos, etc.). El principio es bastante sencillo: cuando se producen condiciones adversas a las ondas de radio, el motor de modulación adaptiva detecta la degradación de la señal y automáticamente cambia el modo de modulación a una tasa inferior, pero más tolerante con el modo de modulación. Es decir, cuando una SS se encuentra cerca de la BS el enlace de radio será mejor, pudiendo ocupar una modulación de mayor orden, lo que se refleja en una mayor tasa de transmisión. [6]

2.2.3.4 Topologías

El estándar 802.16-2004 define dos topologías para los nodos conectados dentro de una red WiMAX:

- Punto a multipunto (PMP)
- Malla (Mesh). También conocida como Multipunto a multipunto (MP-MP)

La principal diferencia entre estos dos modos es la manera en que se llevan a cabo las conexiones. En el modo PMP, el tráfico puede viajar solamente entre la BS y el suscriptor, y por el contrario, en el modo malla, los nodos están conectados entre sí, de modo que aquellos que estén fuera de la cobertura de la BS, puedan establecer una conexión con algún otro nodo y concretar el envío de información hasta ella.

En el entorno de una topología PMP, para que dos nodos puedan establecer una comunicación entre sí, los datos deben viajar necesariamente a través de la BS (BS). Dicha estación utiliza antenas con un ancho de haz relativamente grande dividido en varios sectores que proveen en conjunto una cobertura de 360◦ con una o más antenas. Para lograr la cobertura completa de una zona, frecuentemente se requiere más de una BS, las cuales deben ser conectadas entre sí mediante enlaces de radio, fibra óptica o algún medio similar. Los suscriptores utilizan antenas direccionales apuntando a la BS y compartiendo el canal de radio. Esto se puede lograr mediante varios métodos de acceso como OFDMA, TDMA y CDMA.

Por otro lado, en la configuración malla, cada nodo pueda crear una comunicación con otro nodo sin necesidad de conectarse con la BS previamente. En consecuencia, una de las principales ventajas de esta topología, es que el alcance de una BS se maximiza al poderse comunicar con nodos más lejanos. Sin embargo, el uso del modo mesh, trae consigo las consideraciones pertinentes del ruteo en redes Ad-hoc que escapa al alcance de esta tesis.

2.2.3.5 Propagación NLOS y LOS

La calidad de una transmisión estará afectada por diversos factores, entre ellos, la presencia de obstáculos entre los extremos de la comunicación. Se definen dos tipos de propagación para cualquier tecnología inalámbrica de transmisión de información: transmisión en línea de vista (LOS) y transmisión sin línea de vista (NLOS).

El término LOS se refiere a la propagación de las ondas electromagnéticas viajando con una trayectoria de línea recta, sin obstáculo alguno presente entre el transmisor y el receptor. De acuerdo al estándar, la condición para que una transmisión se considere como LOS, se debe cumplir con que >60% del trayecto de la señal esté libre de obstáculos dentro de la primera zona de Fresnel. [8]

Y, por el contrario, la transmisión NLOS es aquella en la que se presentan obstáculos como edificios, árboles, montañas o líneas de alto voltaje entre el transmisor y el receptor. Esto tiene como consecuencia una señal recibida más débil, ocasionando mala calidad, baja tasa de transmisión o incluso, una posible interrupción en la comunicación.

2.3 802.1Q VLAN

Un enlace troncal es un enlace punto a punto entre dos dispositivos de red que lleva más de una VLAN (Virtual Local Area Network). Un enlace troncal de VLAN permite poder transportar VLANs a través de toda una red.

Un enlace troncal de VLAN no pertenece a una VLAN específica, sino que es un conducto para diferentes VLANs entre switches y routers.

2.3.1 Etiquetado de trama 802.1Q

Los switches al ser dispositivos de Capa 2, sólo utilizan la información del encabezado de trama de Ethernet para enviar paquetes. El encabezado de trama no contiene la información que indique a qué VLAN pertenece la trama. Cuando las tramas de Ethernet se ubican en un enlace troncal, necesitan información adicional sobre las VLAN a las que pertenecen. Esto se logra por medio de la utilización del encabezado de encapsulación 802.1Q. Este encabezado agrega una etiqueta a la trama de Ethernet original y especifica la VLAN a la que pertenece la trama.

2.3.1.1 Visión general del etiquetado de la trama de la VLAN

Cuando el switch recibe una trama en un puerto configurado en modo de acceso con una VLAN estática, el switch quita la trama e inserta una etiqueta de VLAN y envía la trama etiquetada a un puerto de enlace troncal.

Detalles del campo de etiqueta de la VLAN

El campo de etiqueta de la VLAN consiste en un campo EtherType, un campo de información de control de etiqueta y el campo FCS (Frame Check Sequence).

Campo EtherType

Establecido al valor hexadecimal de 0x8100. Este valor se denomina valor de ID de protocolo de etiqueta (TPID). Con el campo EtherType configurado al valor TPID, el switch que recibe la trama sabe buscar la información en el campo de información de control de etiqueta.

Campo información de control de etiqueta

El campo información de control de etiqueta contiene:

- 3 bits de prioridad del usuario: utilizado por el estándar 802.1p que especifica cómo proporcionar transmisión acelerada de las tramas de la Capa 2.

- 1 bit de Identificador de formato ideal (CFI, por sus siglas en inglés): permite que las tramas se transporten con facilidad a través de los enlaces Ethernet.
- 12 bits del ID de la VLAN (VID): números de identificación de la VLAN; admite hasta 4096 ID de VLAN.

Campo FCS

Luego de que el switch inserta los campos de información de control de etiqueta y EtherType, vuelve a calcular los valores FCS y los inserta en la trama.

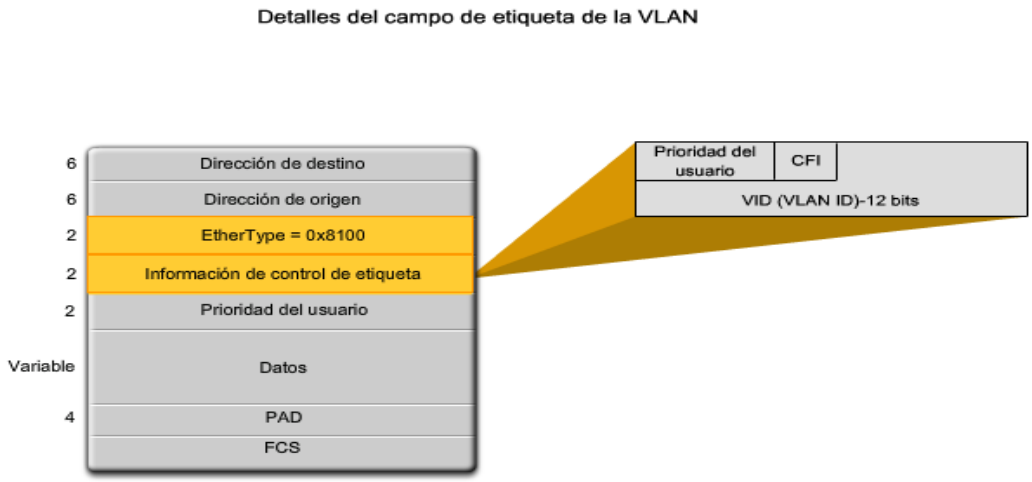


Figura 8 Campo de etiqueta de la VLAN [11]

2.3.5 DTP

El protocolo de enlace troncal dinámico (DTP) es un protocolo propiedad de Cisco. Los switches de otros proveedores no admiten el DTP. El DTP es habilitado automáticamente en un puerto de switch cuando algunos modos de enlace troncal se configuran en el puerto de switch.

El DTP administra la negociación de enlace troncal sólo si el puerto en el otro switch se configura en modo de enlace troncal que admita DTP. El DTP admite los enlaces troncales ISL y 802.1Q.

2.3.6 Modos de enlace troncal

Un puerto de switch en un switch de Cisco admite varios modos de enlaces troncales. El modo de enlace troncal define la manera en la que el puerto negocia mediante la utilización del DTP para configurar un enlace troncal.

A continuación se explica una breve descripción de los modos de enlaces troncales disponibles y la manera en que el DTP se implementa en cada uno.

Activado (de manera predeterminada)

El puerto del switch envía periódicamente tramas de DTP, denominadas notificaciones, al puerto remoto. El comando utilizado es switchport mode trunk. El puerto de switch local notifica al puerto remoto que está cambiando dinámicamente a un estado de enlace troncal. Luego, el puerto local, sin importar la información de DTP que el puerto remoto envía como respuesta a la notificación, cambia al estado de enlace troncal. El puerto local se considera que está en un estado de enlace troncal (siempre activado).

Autodinámico

El puerto de switch envía periódicamente tramas de DTP al puerto remoto. El comando utilizado es switchport mode dynamic auto. El puerto de switch local notifica al puerto de switch remoto que puede establecer enlaces troncales, pero no solicita pasar al estado de enlace troncal. Luego de una negociación de DTP, el puerto local termina en estado de enlace troncal sólo si el modo de enlace troncal del puerto remoto se configuró para estar activo. Si ambos puertos en los switches se configuran en automático, no negocian para estar en un estado de enlace troncal. Negocian para estar en estado de modo de acceso (sin enlace troncal).

Dinámico deseado

Las tramas de DTP se envían periódicamente al puerto remoto. El comando utilizado es switchport mode dynamic desirable. El puerto de switch local notifica al puerto de switch remoto que puede establecer enlaces troncales y solicita al puerto de switch remoto pasar al estado de enlace troncal. Si el puerto local detecta que el remoto se configuró en modo activado, conveniente o automático, el puerto local termina en estado de enlace troncal. Si el puerto de switch remoto está en modo sin negociación, el puerto de switch local permanece como puerto sin enlace troncal.

Desactivación del DTP

Se puede desactivar el DTP para el enlace troncal a fin de que el puerto local no envíe tramas de DTP al puerto remoto. El comando es switchport nonegotiate. Entonces el puerto local se considera que está en un estado de enlace troncal incondicional.

2.3.7 Configurar un enlace troncal 802.1Q

Para configurar un enlace troncal en el puerto de un switch, se usa el comando switchport mode trunk. Cuando se ingresa al modo enlace troncal, la interfaz cambia al modo permanente de enlace troncal y el puerto ingresa a una negociación de DTP para convertir el vínculo a un vínculo de enlace troncal, por más que la interfaz que lo conecte no acepte cambiar.

2.4 Protocolos de VoIP

VoIP

Voip (Voice over Internet Protocol) es un protocolo que permite la transmisión de voz a través de una red IP. Este proceso se lleva a cabo mediante la digitalización, conversión y compresión de la voz a través de paquetes IP, los cuales son encapsulados en RTP (Real-time Transport Protocol), posteriormente en UDP (Protocolo de Datagrama de Usuario) y posteriormente son transmitidos por la red en un paquete IP.

2.4.1 Características VoIP

Ventajas de la voz sobre IP

- Reducir los gastos de desplazamiento y formación, mediante el uso de videoconferencias y conferencias en línea.
- Tener un número de teléfono que suena a la vez en varios dispositivos, para ayudar a los empleados a estar conectados entre sí y con sus clientes.
- Reducir los gastos telefónicos.
- Utilizar una sola red para voz y datos, simplificando la gestión y reduciendo costos.
- En una llamada telefónica normal, la central telefónica establece una conexión permanente entre ambos interlocutores, conexión que se utiliza para llevar las señales de voz. En una llamada telefónica por IP, los paquetes de datos, que contienen la señal de voz digitalizada y comprimida, se envían a través de internet a la dirección IP del destinatario. Cada paquete puede utilizar un camino para llegar, están compartiendo un medio, una red de datos. Cuando llegan a su destino son ordenados y convertidos de nuevo en señal de voz.

Terminología útil relacionada con voz sobre IP

Por voz sobre IP (VoIP) se entiende el método utilizado para transportar llamadas telefónicas sobre una red IP de datos, ya sea que se trate de Internet o de la red interna de una organización. Una de las principales ventajas de la voz sobre IP es la posibilidad de

reducir gastos ya que las llamadas telefónicas se transportan por la red de datos en lugar de la red de la compañía telefónica.

- La telefonía IP incluye el conjunto completo de servicios habilitados por VoIP, como la interconexión de teléfonos para comunicaciones; servicios relacionados como facturación y planes de marcación; y funciones básicas que pueden incluir conferencias, transferencia de llamadas, reenvío de llamadas y llamada en espera.
- Las comunicaciones IP admiten funciones como la mensajería unificada, los centros de atención y conferencias multimedia con voz, datos y vídeo.
- Las Comunicaciones Unificadas elevan a las comunicaciones IP a un nivel superior al utilizar tecnologías SIP (Protocolo de inicio de sesión), junto con soluciones de movilidad, con el fin de unificar y simplificar todas las formas de comunicación, con independencia del lugar, tiempo o dispositivo.

Servicios de voz por IP

Las funciones de voz sobre IP están disponibles en una variedad de servicios. Algunos servicios básicos y gratuitos de voz sobre IP requieren que todas las partes estén en sus computadoras para recibir llamadas. Otros admiten llamadas desde un aparato telefónico tradicional e incluso de un teléfono móvil a cualquier otro teléfono.

Calidad de servicio y seguridad de la voz sobre IP

La mayoría de los servicios de voz sobre IP para el consumidor utilizan Internet pública para realizar llamadas. Pero muchas empresas utilizan voz sobre IP y comunicaciones unificadas a través de sus redes privadas. Eso se debe a que las redes privadas proporcionan una seguridad más robusta y una mejor calidad de servicio que Internet.

2.4.2 Protocolos de señalización

Algunos protocolos utilizados para VoIP son los siguientes: protocolo IP para las decisiones de ruteo, UDP para la entrega de paquetes y RTP/RTCP para transportar en tiempo real.

Los protocolos de señalización son los responsables de localizar una terminal, iniciar y finalizar las llamadas de voz en una red VoIP. Comúnmente existen diferentes protocolos usados en las redes VoIP entre los cuales se encuentran: H.323, MGCP, SCCP y SIP [12].

2.4.2.1 H.323

H.323 puede utilizar hasta dos conexiones TCP y de cuatro a seis conexiones UDP.

Un cliente H.323 inicialmente puede establecer una conexión TCP a un servidor H.323 utilizando el puerto TCP 1720 para solicitar el establecimiento de llamada Q.931. Como parte del proceso de establecimiento de llamada, la terminal H.323 proporciona un número de puerto que el cliente va a utilizar para una conexión TCP H.245. En entornos en donde los gatekeeper H.323 están en uso, el primer paquete se transmite a través de UDP.

Dentro de H.323 se desprenden varios protocolos, los cuales se presentan en la siguiente tabla:

Protocolo	Descripción
H.225	Señalización de llamada
RAS	Registro, admisión y estado de funciones
H.235	Protocolo de seguridad
H.245	Capacidad de negociación
H.450	Servicios suplementarios
H.26x	Códecs de video
G.7xx	Códecs de voz

Tabla 2 Protocolos contenidos dentro de H.323 [13]

2.4.2.2 H.225 (Señalización de control de llamada)

En las redes H.323, los procedimientos de control de llamada están basados en la recomendación H.225 de la UIT (Unión Internacional de Telecomunicaciones), la cual especifica el uso y soporte de los mensajes de señalización Q.931. Un canal confiable de control de llamada es creado a través de la red IP en el puerto TCP 1720. Este puerto es el que inicia los mensajes de control entre dos terminales con el propósito de conectar, mantener y desconectar llamadas.

2.4.2.3 H.245 (Control)

H.245 maneja los mensajes de control de principio a fin entre entidades H.323. Los procedimientos H.245 establecen canales para la transmisión de audio, video, datos e información del canal de control. Una terminal establece un canal H.245 por cada llamada con la terminal participante. Un canal de control confiable es creado en IP usando una asignación dinámica de puerto TCP en el mensaje final de señalización de llamada. El intercambio de capacidades, el abrir y cerrar de los canales lógicos, modos preferentes y mensajes de control se llevan a cabo sobre este canal de control. [13]

2.4.2.4 SIP (Session Initiation Protocol)

SIP es una aplicación de la capa de control (señalización) de protocolo que crea, modifica y termina sesiones con uno o más participantes.Estas sesiones incluyen llamadas telefónicas por Internet, la distribución de multimedia, y conferencias multimedia.

SIP, tal como se define por el IETF, permite las llamadas VoIP. SIP trabaja con Session Description Protocol (SDP) para la señalización de llamadas. SDP especifica los detalles de la corriente de los medios de comunicación. El dispositivo de seguridad puede soportar cualquier SIP (VoIP), puertas de enlace y servidores de VoIP SIP proxy cuando se utiliza. SIP y SDP se definen en estos RFC:

- SIP: Session Initiation Protocol, RFC 3261
- SDP: Session Description Protocol, RFC 2327

SIP soporta tanto sesiones multicast como unicast así como también llamadas punto a punto o multipunto. Para establecer y terminar dichas llamadas se transita por estas cinco facetas SIP:

- Localización de usuario
- Capacidad de usuario
- Disponibilidad de usuario
- Inicio de llamada
- Manejo de llamada

Los componentes principales en un sistema SIP son los agentes de usuario y los servidores de red. Las partes que llaman y las llamadas se identifican por medio de direcciones SIP ya que las partes necesitan localizarse entre sí.

Agente de usuario

El cliente manda las solicitudes SIP y actúa como agente de llamadas de usuario, mientras que el servidor recibe las solicitudes y regresa una respuesta en nombre del usuario, actúa como el agente de usuario llamado.

Servidores de red

Existen dos tipos de servidores SIP: los servidores proxy y servidores de redirección.

- **Servidores Proxy** – Actúa como otros clientes y contiene funciones tanto de cliente como servidor. Un servidor de este tipo es capaz de interpretar y reescribir los encabezados de solicitud antes de enviarlos a otros servidores.

- **Servidores de redirección** – Acepta las solicitudes SIP y envía una respuesta redirigida hacia el cliente con la dirección del siguiente servidor. Estos servidores no aceptan llamadas ni procesan ni envían solicitudes SIP.

2.4.2.4.1 Mensajes SIP

Existen dos tipos de mensajes SIP, las solicitudes iniciadas por los clientes y las respuestas enviadas por los servidores. Cada mensaje contiene un encabezado el cual especifica los detalles de la comunicación. Los mensajes SIP se envían sobre TCP o UDP.

Los encabezados de los mensajes SIP especifican la parte que llama, la parte llamada, ruta y tipo de mensaje de la llamada. [15]

Mensajes de Solicitud

Existen seis solicitudes SIP:

- INVITE – Indica que el usuario o servicio está invitado a participar en una sesión.
- ACK – Representa la confirmación final para concluir la transacción iniciada con
- INVITE.
- OPTIONS – Permite preguntar y recolectar capacidades de agentes de usuario y servidores
- BYE – Usado por las dos partes para liberar una llamada.
- CANCEL – Sirve para cancelar cualquier solicitud en progreso
- REGISTER – Registra la locación de clientes con los servidores SIP.

Mensajes de respuesta

Son los mensajes enviados en respuesta a una solicitud e indican el éxito o fallo de lallamada, incluyendo el estado del servidor.

Operación básica de SIP

Los servidores SIP manejan las solicitudes de dos maneras y la operación de estas se basaen invitar a un participante a la llamada. Los dos modos de operación del servidor SIP son:los modos de servidor proxy y el de servidor de redirección. [15]

Los pasos para llevar a cabo una llamada de dos vías en el modo proxy son los siguientes:

- El servidor proxy acepta la solicitud INVITE del cliente.
- El servidor proxy identifica la localización usando las direcciones suministradas y los servicios de locación.

- Una solicitud INVITE es emitida hacia la locación obtenida.
- El agente de usuario de la parte llamada alarma al usuario y regresa una indicación de éxito al servidor proxy involucrado.
- Una respuesta de OK se envía del servidor proxy a la parte que llama.
- La parte que llama confirma mediante una petición ACK, la cual se envía por el servidor proxy hacia la parte llamada.

2.4.3 Protocolos de Transporte

Sobre IP recaen dos tipos de tráfico: los de UDP y los de TCP. Al usar TCP se tendrá una conexión confiable en comparación con UDP.

Debido a que el tráfico de voz es muy sensible a los retrasos de tiempo, la solución más lógica es usar UDP/IP para transportar la voz. La IETF adoptó RTP para tiempo real o sensibilidad al retardo. VoIP viaja en la parte superior de RTP, el cual viaja en la parte superior de UDP. Por lo tanto VoIP es transportado con un encabezado de paquete RTP/UDP/IP como se muestra en la figura. [17]

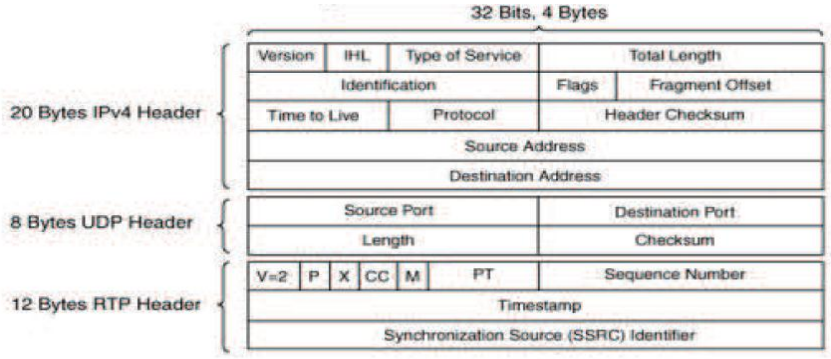


Figura 9 Encabezados de protocolos RTP, UDP e IP

2.4.3.1 RTP (Real-Time Transport Protocol)

RTP es un estándar de la IETF RFC 1889 y 3050 para la entrega unicast y multicast de voz y video. El protocolo de transporte que usa RTP es casi siempre UDP pero es un servicio no confiable basado en el mejor esfuerzo y aunque puede llegar a sonar como algo perjudicial en realidad es el mejor método para transportar este tipo de datos.

UDP al ser un servicio basado en el mejor esfuerzo no intenta retransmitir ni reordenar paquetes como lo haría TCP. La explicación de por qué UDP es la mejor opción para transporte es simple: si tratáramos de retransmitir un paquete de voz perdido, al hacerlo y que el paquete alcanzara su destino, el sonido contenido no tendría sentido pues estaría siendo entregado fuera de tiempo.

RTP por medio de su encabezado proporciona un campo llamado “timestap” el cual se pone en cada paquete de voz digitalizada y ayuda a corregir el problema de retardo de llegada.

2.4.3.2 cRTP (Compress RTP)

cRTP es una opción que surgió para mitigar un poco el problema que aún se tenía al utilizar RTP, debido a que la voz es muy sensible al retardo. cRTP toma los 40 bytes del conjunto de encabezados y los corta entre dos y cinco bytes [17].

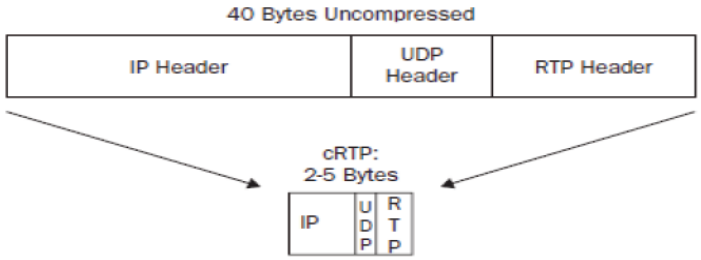


Figura 10 RTP a cRTP

Lo que hace cRTP es que una vez que la información es conocida en los dos extremos del cable y ya que mucha de la información contenida en los encabezados UDP/IP/RTP es estática, cRTP quita esa información y al no enviar esta información se conserva ancho de banda. Este protocolo es más eficiente en enlaces WAN con velocidades T1 y menores, enlaces con mayores velocidades no obtienen beneficio alguno.

2.4.4 Códecs

VoIP funciona digitalizando la voz en paquetes de datos, enviándola a través de la red, se realiza la reconversión de digital a analógica en la terminal de destino de la comunicación. La señal análoga del teléfono es digitalizada en señales PCM25 por medio del codificador/decodificador de voz.

Las muestras PCM (Pulse Code Modulation) pasan por el algoritmo de compresión, el cuál comprime la voz y la fracciona en paquetes que pueden ser transmitidos en la red WAN (Wide area Network). Al otro extremo del canal de comunicación se realiza el proceso inverso.

Los códecs son usados dentro del mundo VoIP para codificar y decodificar los datos de voz. Estos códecs nos pueden ayudar a usar menor número de bits por conversación de voz, por lo que se traduce en mayor número de llamadas simultáneamente en un ancho de banda finito. La compresión tiene como objetivo eliminar la redundancia de los datos que son enviados. Usualmente entre más comprimida sea la señal de voz más recursos usará el DSP, por lo que estos códecs se clasifican por su complejidad.

2.4.4.1 ITU G.711

Este estándar también se conoce como PCM. Este códec muestrea la señal de voz a una frecuencia de 8 000 muestras por segundo. Esto proporciona una mejor calidad a comparación de la mayoría de los códecs empleados.

Una llamada telefónica requiere 64 Kbps en el cable. De acuerdo al teorema de muestreo de Nyquist tendremos 8 000 muestras de voz cada segundo. Cada muestra es de 8 bits; por lo que al multiplicar 8 000 x 8, obtendremos 64 Kbps, lo que significa que G.711 no usa compresión y es la alternativa cuando existe suficiente ancho de banda. [17]

2.4.4.2 ITU G.729

El muestreo que provee este códec es el mismo que el de G.711. La diferencia de G.711 radica en la compresión, pues G.729 usa una técnica llamada CS-ACELP26 la cual se basa en métodos alternos de muestreo y expresiones algebraicas como libro de códigos para predecir la representación numérica real. Estas expresiones algebraicas se envían al sitio remoto, donde estas son decodificadas y el audio es sintetizado para imitar el audio original; la predicción y sintetización de forma de onda de audio degrada la calidad de la señal de voz haciendo que la voz del que habla suene robótica.

La ventaja de este códec es que permite una compresión de voz que sólo requiere de 8 Kbps por llamada en vez de los 64 Kbps requeridos por el G.711. Esto significa que se podrían hacer ocho llamadas en el espacio de una que estuviera usando G.711, lo que sería bueno para compensar el despliegue de VoIP en un enlace WAN de poca rapidez. [18]

2.5 Estándares MPEG

EL archivo de video digital tiene tres componentes básicos:

a) Señal de video (codificada)

b) Señal de audio (codificada)

c) Contenedor (encapsulación)

La codificación de las señales puede ser de un formato analógico hacia uno digital o directamente entre formatos digitales.

Cuando el origen es un formato analógico el objetivo de codificar es convertir la información para que pueda ser procesada por las computadoras.

Cuando la fuente es digital el proceso se denomina transcodificación, el objetivo de dicha operación puede ser obtener compatibilidad entre el formato y una aplicación en

particular, también puede ser para obtener una mayor calidad de video ó como en nuestro caso reducir la tasa de reproducción.

El contenedor o envoltura es la estructura responsable de coordinar la señal de video con la señal de audio, además de proveer funciones extras que ayudan a la reproducción del contenido, dichas funciones van desde agregar subtítulos, hasta corrección de errores para en medios con pérdidas (para soportar el streaming).[9]

MPEG (Moving Pictures Experts Group) es un grupo de trabajo de ISO e IEC, este se encarga del desarrollo de estándares de video, es decir de normalizar los códecs y contenedores. Desde su creación ha desarrollado una gran cantidad de códecs como son:MPEG-1, MPEG-2, MPEG-3, MPEG-4, MPEG-7, MPEG-21, MPEG-A, MPEG-B, MPEG-C, MPEG-D, MPEG-E, MPEG-F y MPEG-4AVC. En cuestión de formatos contenedores cuenta actualmente con tres tipos: MP4, MPEG-TS y MPEG-PS.

A partir de las opciones de códecs de transcodificación disponibles en nuestro software (VLC) y de la calidad de la imagen observada elegimos usar la codificación MPEG 4 AVC y el contenedor tipo MPEG-TS, este último elegido por la capacidad de operar con pérdidas de paquetes.

2.6 FTP (File Transfer Protocol)

El tráfico de datos se refiere al flujo de información que contiene por ejemplo: la estructura de una página web, texto, imágenes, etc. Este tipo de información una vez recibida se mantiene estática así que lo importante es recibir todos los datos y sin errores, también debe mencionarse que este tipo de flujo no es afectado por retardos. Por lo anterior la transmisión de datos se realiza bajo conexiones TCP ya que, TCP es capaz de corregir errores y solicitar retransmisiones.

FTP es un servicio (basado en el protocolo del mismo nombre) de transferencia de archivos, forma parte del conjunto de protocolos TCP/IP por lo que garantiza la compatibilidad con el resto de aplicaciones y dispositivos de la red.

Dicho servicio se basa en el modelo cliente-servidor, el servidor es el encargado de almacenar los archivos a los que se accede de manera remota, también maneja una base de datos con las cuentas de los clientes aceptados y los permisos de estos sobre los archivos. La función del cliente se limita a autentificarse y copiar archivos hacia su ubicación o viceversa (si el servidor lo permite). [10]

El uso de un servidor FTP para simular el tráfico de datos nos ayuda a evaluar el desempeño del enlace, por cumplir con las siguientes características:

a) FTP se basa en conexiones TCP por lo que comprobar la integridad de un archivo descargado a través del enlace nos indicaría sí el enlace soporta tráfico de datos.

b) FTP está diseñado para transmitir a la máxima tasa que le permita el medio de transmisión, esto nos ayuda a evaluar sí las políticas de calidad a partir de la degradación de la calidad en la transmisión de voz y video cada vez que se está descargando un archivo.

CAPÍTULO III

Equipo de red

Se brinda una breve descripción de las capacidades de los equipos de red usados (swithces, routers, BS y SS), posteriormente se explica cómo se realiza en general la configuración de dichos equipos.

El “Gateway de voz” representa un caso particular puesto que es un switch pero además posee un servidor integrado que regula la comunicación entre los teléfonos IP. Considerando estos últimos cómo el servicio decidimos incluir el “Gateway de voz” en este capítulo.

3.1 BS WiMAX Redline 100AN-U

El sistema WiMAX utilizado está compuesto por la BS marca redline modelo 100AN-U, estaciones suscriptoras de uso interior (SUI), y estaciones suscriptoras de uso exterior (SUO).

3.1.1 Características

La BS cumple con la especificación IEEE 802.16-2004, es decir WiMAX fijo. Soporta transmisiones punto a punto, y punto a multipunto ambas NLOS. Está compuesta por la unidad interior (IDU) y la unidad exterior (ODU). La primera se encarga de recibir y procesar el flujo de datos que ingresa por el puerto ethernet, tiene la apariencia de un ruteador sólo que una de sus interfaces permite la conexión de un cable coaxial el cual alimenta la ODU. La ODU contiene el modem y la antena, esta es sectorial de 60 grados con una ganancia de 17 dBi y polarización vertical. [8]

El IDU y ODU aparecen en la siguiente imagen:

Figura 11 BS WiMAX [8]

Soporta un ancho de banda de 3.5 MHz ó 7 MHz (especificación WMAN-OFDM) en la banda de 3.4 a 3.6 GHz. En teoría pueden existir hasta 28 canales de 7 MHz o 57 de 3.5 MHz; Sin embargo se necesita una BS por canal. [8]

El funcionamiento de la BS puede verse como un acces point de kilómetros de cobertura, además analiza el contenido del flujo de datos que recibe y basado en parámetros preconfigurados por el administrador permite y coordina el acceso al canal inalámbrico. También administra el acceso al medio inalámbrico en las estaciones suscriptoras para que respeten las mismas políticas que la BS.

El sistema soporta transmisiones sin línea de vista (NLOS), con línea de vista (LOS) y con línea de vista óptica (OLOS). El enlace con línea de vista se refiere a una transmisión sin obstáculos en al menos el 60% de la zona de Fresnel. En el enlace OLOS pueden existir obstáculos dentro de esta zona pero aun así existe visibilidad entre la antena de la BS y la SS.

3.1.2 Administración de las políticas de calidad

Service Class (SC):

Cómo se mencionó la subcapa MAC utiliza el mecanismo de "schedulling" o planificación para el manejo y la entrega de las SDU y las MAC PDU con diferentes requerimientos de QoS.

Para elegir el mecaniso de "schedulling" redline definió una plantilla denominada "SC". Con dicha plantilla se crean las políticas de calidad que debe cumplir el enlace.

La plantilla de "SC" necesita que le sea asignado un nombre y un tipo de "schedulling", estos son los definidos en el estándar 802.16-2004 (rTPS, nrTPS, UGS, BE) y se describen a continuación:[8]

Unsolicited Grant Service (UGS)

UGS está diseñado para soportas paquetes de datos de tamaño fijo a una tasa constante de bits (CBR). Ejemplos de algunas aplicaciones que pueden utilizar estos servicios son la emulación de T1/E1 y VoIP sin la supresión de silencio. UGS ofrece porciones de tamaño fijo en una base periódica de tiempo real y no necesita la SS para pedir explícitamente ancho de banda.

real-time Polling Service (rtPS)

Este servicio está diseñado para soportar flujos de servicio en tiempo real, tales como videos MPEG, que generan paquetes de datos de tamaño variable en una base periódica. En ésta clase de servicio, la radio-base provee oportunidades de petición unicast para la petición de ancho de banda a la SS.

Non-real-time Polling Service (nrtPS)

Este servicio está diseñado para soportar flujo de datos tolerantes al retraso, tales como un FTP, que requiere porciones de datos de tamaño variable a una tasa mínima garantizada. En nrtPS se permite tener oportunidades de petición Unicast, pero el promedio de

duración entre dos de éstas oportunidades está en el orden de unos cuantos segundos, que es más grande comparado con rtPS.

Best Effort (BE)

Este servicio está diseñado para soportar lujo de datos que no requieran un estricto soporte de QoS, tales como navegar por la red. Los datos son enviados cuando los recursos están disponibles y no se requieren para otra clase de servicios que ya estaban programadas.

Extended real-time Polling Service(ertPS)

ertPSestá diseñado para funcionar exclusivamente con el estándar IEEE 802.16-2005d, soporta aplicaciones en tiempo real, como VoIP con supresión de sonido, que tengan tasa de datos variables pero que requieran una tasa de datos y retraso garantizados.

Una vez asignado el tipo de "schedulling" se activan las siguientes opciones en la plantilla:

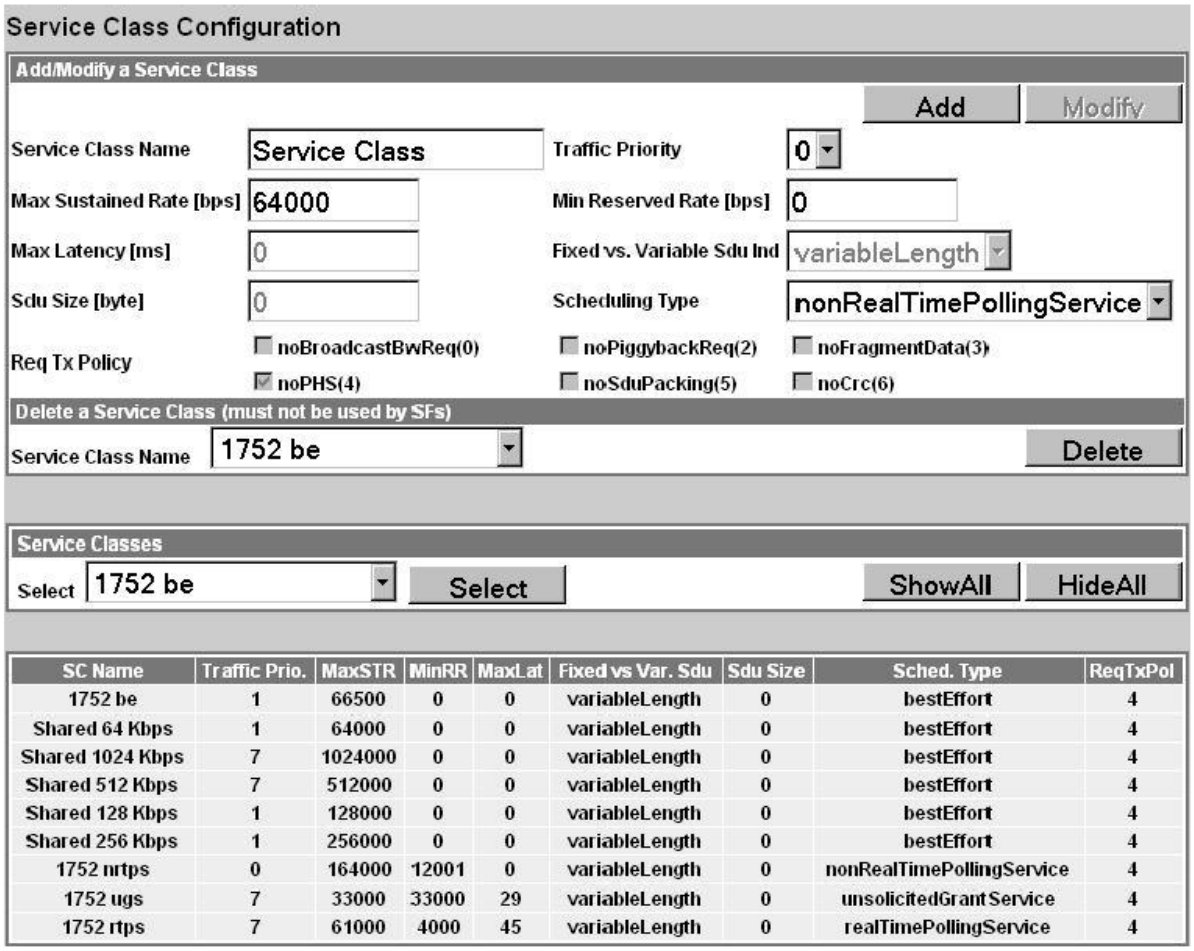
Prioridad (Traffic Priority): Indica la preferencia que tendrá el flujo de datos basado en este tipo de "SC" sobre otros flujos que utilicen el mismo tipo de "schedulling". La mayor prioridad está representada por el número siete y la menor por el cero.

Tasa máxima/mínima: (Max/Min Sustained rate): Indica los límites máximo y mínimo en la tasa de transmisión del flujo de datos basado en la "SC".

Sdu: Es la opción para elegir en recibir paquetes de longitud varibale en el puerto ethernet. Si se activa la opción debe definirse el tamaño máximo de los paquetes en la casilla del mismo nombre (sdu size).

Req Tx Policy: sirve para elegir cómo se realizarán las peticiones y asginación del canal inalámbrico.

La figura siguiente es la captura de pantalla de la interfaz para configurar las SC:



SC Name	Traffic Prio.	MaxSTR	MinRR	MaxLat	Fixed vs Var. Sdu	Sdu Size	Sched. Type	ReqTxPol
1752 be	1	66500	0	0	variableLength	0	bestEffort	4
Shared 64 Kbps	1	64000	0	0	variableLength	0	bestEffort	4
Shared 1024 Kbps	7	1024000	0	0	variableLength	0	bestEffort	4
Shared 512 Kbps	7	512000	0	0	variableLength	0	bestEffort	4
Shared 128 Kbps	1	128000	0	0	variableLength	0	bestEffort	4
Shared 256 Kbps	1	256000	0	0	variableLength	0	bestEffort	4
1752 nrtps	0	164000	12001	0	variableLength	0	nonRealTimePollingService	4
1752 ugs	7	33000	33000	29	variableLength	0	unsolicitedGrantService	4
1752 rtps	7	61000	4000	45	variableLength	0	realTimePollingService	4

Figura 12 Menú de SC [8]

Service Flow (SF)

Con la "SC" se definen los parámetros que debe cumplir la tasa de transmisión, lo siguiente que debe indicarse es el sentido del flujo y en que campos del paquete deben buscarse las coincidencias para acceder al flujo de datos asociado a la "SC". La plantilla que realiza este mapeo se denomina "SF".

La plantilla definida en la BS permite relacionar la "SC", con un flujo unidireccional y los campos a analiza en la trama ethernet recibida. Los campos de la plantilla son:

SFID: número que actúa como la huella digital del "SF", es decir identifica al "SF" y cumple con ser diferente de todas las demás.

SSName: Es la dirección MAC de la SS con la cual se establecerá el enlace.

Dirección: Indica el sentido de la transmisión. "Downstream" se refiere al flujo que va de la BS al suscriptor, y "upstream" identifica el sentido opuesto.

SCName: Es el campo mediante el cual se asocia la "SC" al "SF", en él se debe seleccionar el nombre de la "SC" a utilizar.

CSespecification: Indica el campo en el que se debe buscar la coincidencia en el flujo de datos recibido por el puerto ethernet. En esta opción se aprecia la gran compatibilidad de WiMAX con los demás protocolos basados en IP ya que además de admitirse el procesamiento en base al encabezado el paquete IP se puede hacer también respecto al encabezado ethernet, al de VLANs (802.1Q) y combinaciones de estos.

Es importante mencionar la existencia de "default SFs". Los equipos de red intercambian información entre sí para establecer la conexión por ejemplo al mapear direcciones MAC con direcciones IP (ARP). Los paquetes sobre los cuales viajan dicha información tienen un formato que impide que sus campos coincidan con los declarados para acceder a la interfaz aérea. Al no intercambiarse dichos paquetes se pierde la comunicación en capa 3 puesto que no pueden completarse las tablas ARP.

Los "default SFs" son los encargados de transportar dicho tráfico, el "default SFs" de bajada se encuentra siempre activado; Sin embargo el de subida el de subida debe activarse mediante la configuración avanzada del sistema.

La figura siguiente es la captura de pantalla de la interfaz para configurar los SFs:

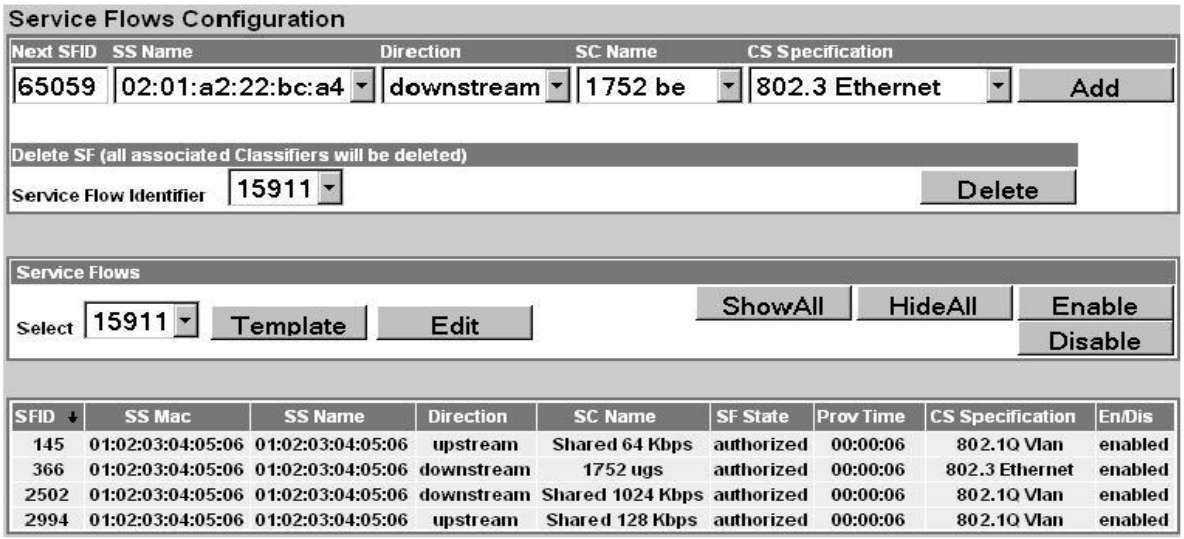


Figura 13 Menú de SFs [8]

Classifiers

Los clasificadores toman un determinado "SF" como argumento de entrada y en base al protocolo de red especificado proporciona una interfaz para ingresar los valores que debe contener el encabezado del paquete. En caso de elegir el protocolo IP pueden ingresarse las direcciones IP origen y destino, sus máscaras de red y el número de puerto.

La BS tiene la capacidad de crear dinámicamente tantos clasificadores como dispositivos finales se posean; Sin embargo su uso limita el uso de las políticas de calidad puesto que estas se asignan al suscriptor impidiendo así especificar el servicio o el usuario al que se desea dar prioridad, además se restringe a usar direcciones IP del mismo segmento.

El proceso para activar esta funcionalidad consiste en crear la SC, mapearla con un SF y finalmente agregar el SF a un clasificador genérico, este es un clasificador con sólo el valor de la prioridad especificada. Además al momento de agregar un suscriptor (el proceso se detalla más adelante) debe activarse la etiqueta MAC learning.

La figura siguiente es la captura de pantalla de la interfaz para configurar los clasificadores:

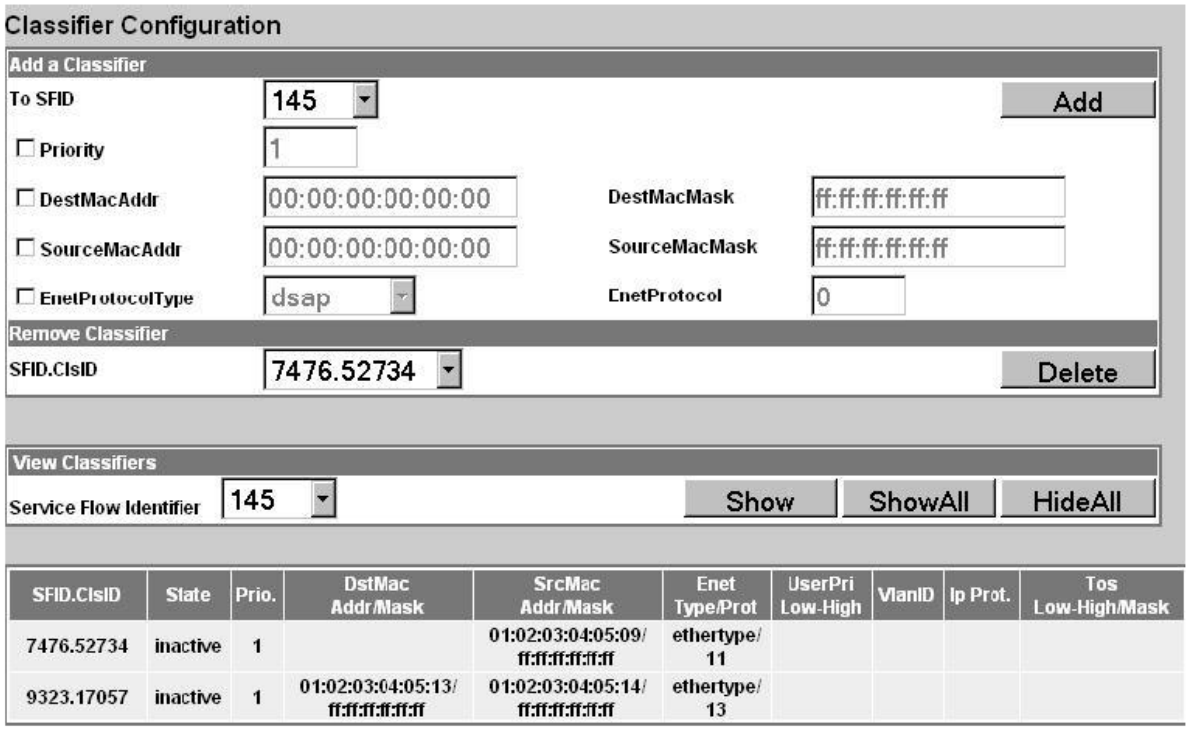


Figura 14 Menú de clasificadores [8]

Resumiendo la BS redline 100AN-U cuenta con las siguientes plantillas para definir la calidad de servicio:

La siguiente tabla resume las características de las plantillas usadas por WiMAX:

SC	Define la tasa de transmisión a la que debe someterse el flujo de datos, así como los valores de retrdo tolerado y la prioridad sobre otros flujos.
SF	Mapea la SC a una SS, indica el sentido del flujo y sobre que encabezado se basa clasificación.
Classifier	Especifica los valores esperados en el encabezado.

Tabla 3 Plantillas de WiMAX

3.1.3 Parámetros de la interfaz aérea

Cómo se mencionó anteriormente la BS es capaz de operar con canales de 3.5 MHz y de 7 MHz, la selección de dicho parámetro, así como el del prefijo cíclico, y la frecuencia de operación (central) se realiza desde la opción "Wireless Interface Configuration" de la interfaz gráfica (el accesoa la interfaz gráfica se describe más adelante). Además es posible usar el control de potencia y ganancia automático en las estaciones suscriptoras.

Para usar el control automático de potencia (de transmisión) debe activarse la etiqueta con el mismo nombre en la BS e ingresar el nivel de potencia promedio esperado de la señal recibida, los valores sugeridos son de -75 dBm para el canal de 3.5 MHz y -72 dBm para el canal de 7MHz.

Para activar el control automático de ganancia se activan las casillas con este nombre tanto en la BS como en los suscriptores,

3.1.4 Administración del equipo:

Para acceder a la interfaz gráfica se conecta una computadora a la BS mediante un cable de red (directo), luego seasigna una dirección IP del mismo segmento (192.168.182.X/24 por defecto) de la BS a la computadora. Cuando la conexión está lista se abre un navegador web y en el campo de la URL se ingresa la dirección 192.168.182.3 (dirección por defecto de la BS). El navegador pide entonces un nombre de usuario y contraseña, ambos son "admin". [8]

Lo siguiente es agregar un suscriptor, para ello se da click a la pestaña "Suscriber", al hacerlo se abre una página donde se debe ingresar la dirección MAC del suscriptor que actua cómo su identificador puesto que es única, además se le da un nombre y de quererse se activa la opción para que el suscriptor aprenda las direcciones MAC de los dispositivos

conectados a él. Cómo el objetivo de nuestro enlace es brindar calidad de servicio basado en la dirección IP no activamos dicha casilla. La siguiente figura muestra el menú descrito:

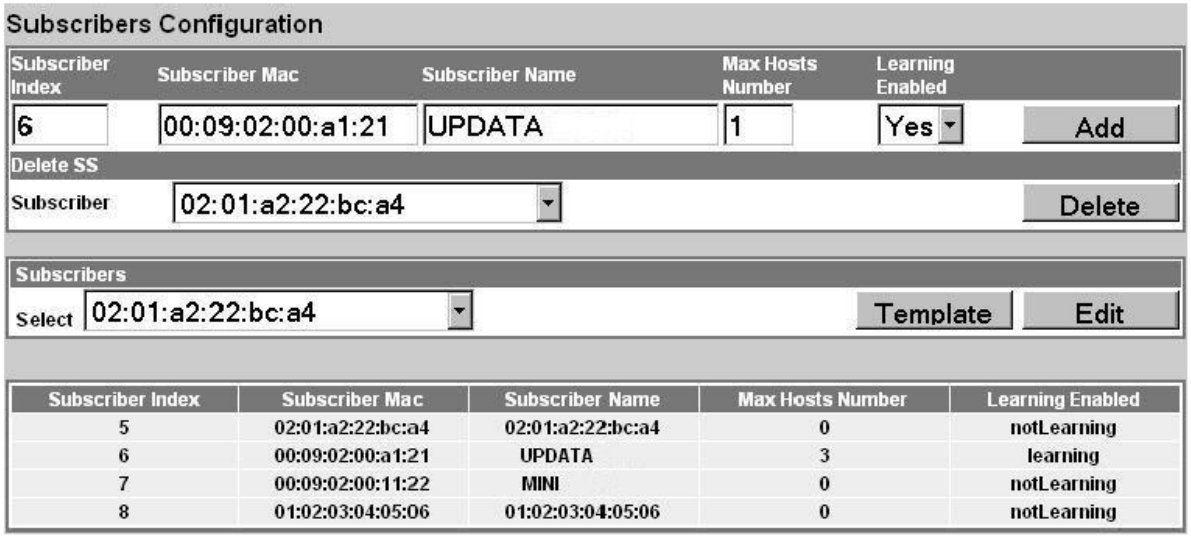


Figura 15 Menú de suscriptores [8]

Después de agregar el suscriptor se sigue el proceso descrito anteriormente, enumerando los pasos tenemos:

1) Crear la SC

2) Mapear en SF la SC, el suscriptor hacia el cual se dirige el flujo, la dirección del flujo y el encabezado en base al que se realiza el filtrado.

3) Se crea un clasificador basado en el SF, en este se especifican los valores del encabezado.

Para activar el "uplink default SF" dentro de la interfaz gráfica se ingresa a la pestaña de configuración avanzada, el sistema pide otro nombre de usuario y contraseña que en este caso son: redline y guest respectivamente. Dentro del menú se activa la opción de UL SF default y en la ventana debajo de esta se ingresa la tasa de transmisión de dichos SFs (se crea uno por suscriptor que esté dado de alta). [8] La siguiente figura corresponde al menú para modificar la configuración avanzada:

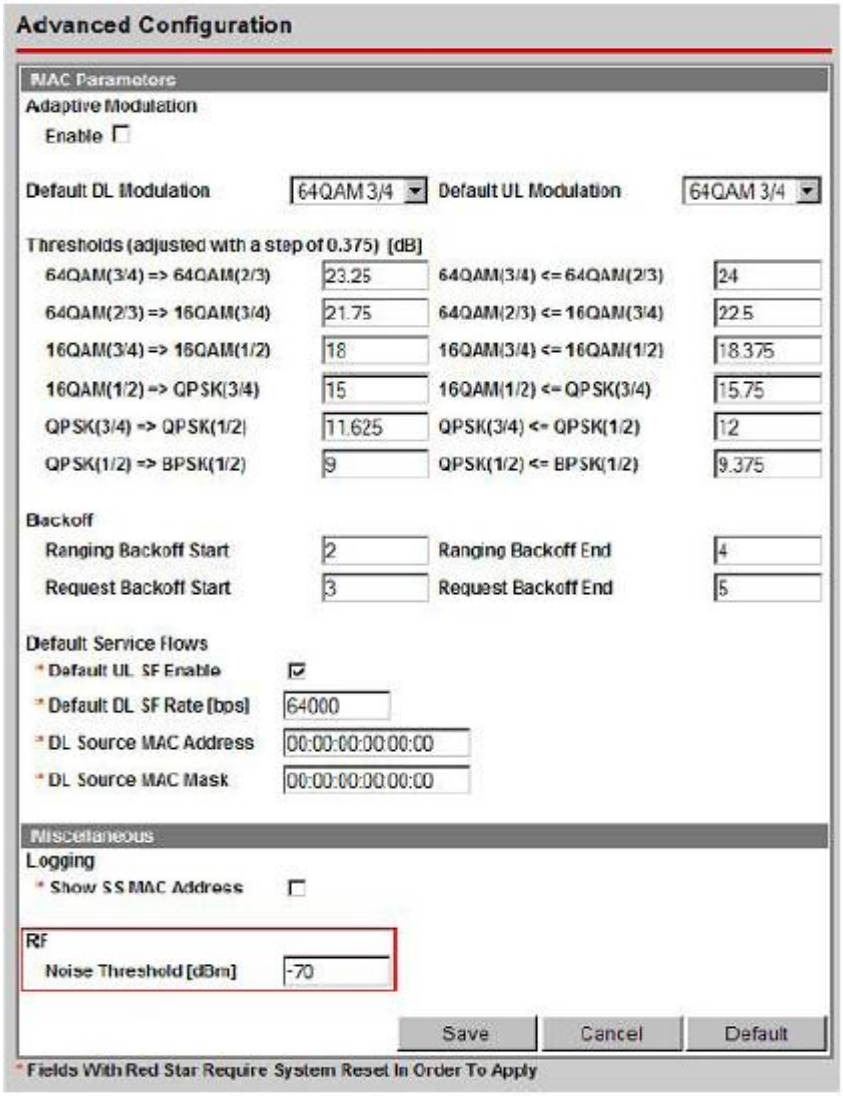


Figura 16 Menú de configuración avanzada [8]

3.2 Estaciones Suscriptoras

Redline fabrica dos tipos de sistemas estaciones suscriptoras, una para uso en el interior de las construcciones (SUI) y otra para su uso fuera de ellas (SUO).

3.2.1 SUI

La antena, el modem y el equipo encargado de procesar las tramas entre la interfaz aérea y el puerto ethernet se encuentran integrados en una sola pieza. Esta se alimenta mediante un transformador CA-CD a 5 [V]. La antena es sectorial de 80 grados, tiene 10.5 dBi de ganancia, opera de 3.3 a 3.8 GHz y tiene polarización horizontal y vertical. Físicamente el SUI es como se muestra en la siguiente figura:[19]

Figura 17 SUI [19]

3.2.2 SUO

La unidad SUO aparenta ser solamente una antena; Sin embargo también posee la unidad de procesamiento integrada. Está diseñada para operar a la intemperie por lo que se alimenta por el puerto ethernet a través de PoE (Power over Ethernet). Su antena es más robusta siendo de 13.5 grados con una ganancia de 20 dBi, también cuenta con polarización horizontal y vertical. [19]

3.2.3 Administración del equipo:

Los flujos de datos admitidos en el radioenlace así como sus características se configuran automáticamente en las estaciones suscriptoras mediante la descarga de los clasificadores. Siendo así lo único que debe configurarse es la interfaz aérea, y la dirección IP. Opcionalmente pueden activarse el control automático de potencia y el control automático de ganancia.

Establecer la interfaz aérea consta de elegir los valores límites del barrido de frecuencia que realiza el suscriptor para encontrar la banda en la que opera la BS. También se selecciona el ancho de banda del canal (que debe coincidir con el seleccionado en la BS) y la selección de la longitud del prefijo cíclico.

El direccionamiento IP consta de establecer la dirección IP y la máscara de default. Habilitar o deshabilitar la casilla de ethTag para el envío de tramas basadas en VLAN y habilitar o deshabilitar la casilla SSmanaged para la administración del direccionamiento vía IP.

Las unidades suscriptoras tienen la desventaja de no tener interfaz gráfica, deben administrarse vía telnet, el cual es un servicio que de acceso a una línea de comandos para configurar la unidad.

Se accede al servicio de telnet conectando el SUI o SUO a una computadora como en el caso de la BS, luego en la computadora se abre una línea de comandos y se ingresa: [19]

>telnet 192.168.101.1

La dirección IP está fijada en el equipo y es una medida de seguridad por sí se olvidara la IP asignada por el administrador.

Habiendo ingresado al sistema hay una interfaz global desde la cual se puede acceder a todos los parámetros. En este caso empezamos por modificar los referentes a la interfaz aérea para ello se ingresa a la carpeta respectiva:

>rfConfig

Dentro de la carpeta se encuentran las variables que definen los límites inferior y superior del barrido en frecuencia, se asignan los valores deseados mediante los comandos:

>set LoRfFreq1 límite_inferior_Hz

>set HiRfFreq1 límite_superior_Hz

Se sale de la carpeta con el comando:

>exit

Luego se ingresa a la carpeta de la capa física, se asigna el valor del ancho de banda y la duración del prefijo cíclico:

>phyConfig

>set cyclicPrefix a

>set bandWith b

>exit

La variable a puede valer 1/4, 1/8, o 1/16, mientras que b puede ser 3500 ó 7000.

Para activar el control automático de ganancia se vuelve a ingresar la carpeta de lainterfaz aérea y se habilita la etiqueta respectiva:

>rfConfig

>set RxAgc 1

Para configurar los parámetros IP se ingresa a la interfaz global, y se asignan los valores de la dirección y la máscara:

>set ipAddress Address a.b.c.d

>set ipAddress Mask e.f.g.h

Finalmente debe desactivarse la administración de tramas VLAN y el dhcp, dichas etiquetas se desactivan desde el modo de configuración global:

>set managedSS 0

>set ethTag 0

3.4 Switch CISCO serie Catalyst 2960

3.4.1 Switch

Un Switch es un dispositivo que se encarga de filtrar, reenviar o inundar tramas basándose en la dirección destino de cada trama. El Switch opera en la capa de enlace de datos del modelo OSI.

3.4.2 Características de los Switches Catalyst 2960

Los switches de la serie Catalyst 2960 habilitan las redes de capa de entrada de empresas medianas y de sucursales para prestar servicios de LAN mejorados. Los switches de la serie Catalyst 2960 son apropiados para las implementaciones de la capa de acceso en las que el acceso a la fuente de energía y al espacio es limitado.

Los switches de la serie Catalyst 2960 ofrecen lo siguiente:

- Velocidades de reenvío desde 16 Gb/s a 32 Gb/s
- Conmutación de capas múltiples
- Características de QoS para admitir comunicaciones IP
- Listas de control de acceso (ACL, Access control lists)
- Conectividad Fast Ethernet y Gigabit Ethernet
- Hasta 48 puertos de 10/100 o puertos de 10/100/1000 con enlaces gigabit adicionales de doble propósito

3.4.3 VLAN

Una LAN virtual (VLAN) permite crear grupos de dispositivos conectados a la red de manera lógica que actúan como si estuvieran en su propia red independiente, incluso si comparten una infraestructura común con otras VLAN. Cuando se configura una VLAN, se le puede poner un nombre para describir la función principal de los usuarios de esa VLAN. Las VLAN permiten que el administrador de la red implemente las políticas de acceso y seguridad

para grupos particulares de usuarios. Por ejemplo como se muestra en la figura: se puede permitir que el cuerpo docente, pero no los estudiantes, obtenga acceso a los servidores de administración de ingeniería [11].

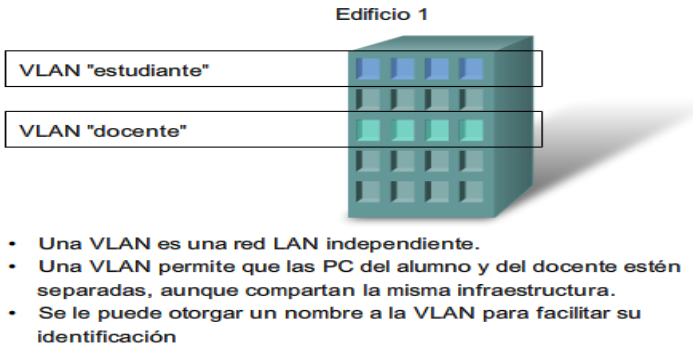


Figura 18 Ejemplo de aplicación de VLANs

3.4.4 Tipos de VLAN

3.4.4.1 VLAN de datos

Una VLAN de datos es una VLAN configurada para enviar sólo tráfico de datos generado por el usuario. Una VLAN podría enviar tráfico basado en voz o tráfico utilizado para administrar el switch, pero este tráfico no sería parte de una VLAN de datos. Es una práctica común separar el tráfico de voz y de administración del tráfico de datos. La importancia de separar los datos del usuario del tráfico de voz y del control de administración del switch se destaca mediante el uso de un término específico para identificar las VLAN que sólo pueden enviar datos del usuario: una "VLAN de datos". A veces a una VLAN de datos se le denomina VLAN de usuario.

3.4.4.2 VLAN nativa

Se asigna una VLAN nativa a un puerto troncal 802.1Q. Un puerto de enlace troncal 802.1 Q admite el tráfico que llega de muchas VLAN (tráfico etiquetado) como también el tráfico que no llega de una VLAN (tráfico no etiquetado). El puerto de enlace troncal 802.1Q coloca el tráfico no etiquetado en la VLAN nativa.Una VLAN nativa sirve como un identificador común en extremos opuestos de un enlace troncal [11].

3.4.4.3 VLAN de administración

Una VLAN de administración es cualquier VLAN que se configura para acceder a las capacidades administrativas de un switch. La VLAN 1 serviría como VLAN de administración si no definió proactivamente una VLAN única para que sirva como VLAN de administración. Se asigna una dirección IP y una máscara de subred a la VLAN de administración. Se puede

manejar un switch mediante HTTP (Hyper Text Transfer Protocol), Telnet, SSH (Secure Shell) o SNMP (Simple Network Management Protocol).

3.4.4.4 VLAN de voz

La VLAN de voz se utiliza de forma independiente a las VLAN de datos, en donde esta VLAN se encarga de transportar la voz teniendo en consideración las siguientes especificaciones.

El tráfico de VoIP requiere:

- Ancho de banda garantizado para asegurar la calidad de la voz
- Prioridad de la transmisión sobre los tipos de tráfico de la red
- Capacidad para ser enrutado en áreas congestionadas de la red
- Demora de menos de 150 milisegundos (ms) a través de la red

3.4.5 Configuración de VLAN

La siguiente tabla muestra los comandos para la configuración de una VLAN, así como una descripción de estos.

Sintaxis de comando de la CLI del IOS de Cisco	
Cambiar de modo EXEC privilegiado a modo de configuración global.	`S1#configure terminal`
Crear una VLAN. El id de la VLAN es el número de VLAN que se creará. Switches para el modo de configuración de VLAN para el vlan id de la VLAN.	`S1(config)#vlan id de la VLAN`
(Opcional) Especificar un único nombre de VLAN para identificar la misma. Si no se ingresa ningún nombre, el número de la VLAN, relleno con ceros, se anexa a la palabra 'VLAN', por ejemplo, VLAN0020.	`S1(config-vlan)#name nombre de la VLAN`
Volver a modo EXEC privilegiado. Debe finalizar su sesión de configuración para que la configuración se guarde en el archivo vlan.dat y para que la configuración entre en vigencia.	`S1(config-vlan)#end`

Tabla 4 Configuración de una VLAN [11]

3.4.6 Asignar un puerto de switch

Una vez que haya creado una VLAN, se asigna uno o más puertos. Cuando se asigna un puerto de switch a una VLAN en forma manual, se le conoce como puerto de acceso estático. Un puerto de acceso estático puede pertenecer a sólo una VLAN por vez.

La siguiente tabla muestra la configuración de un puerto de acceso en un Switch.

Sintaxis del comando de la CLI del IOS de Cisco	
Ingrese el modo de configuración global.	`S1#configure terminal`
Ingresar la interfaz para asignar la VLAN.	`S1(config)#interface` *id de la interfaz*
Definir el modo de asociación de VLAN para el puerto.	`S1(config-if)#switchport mode access`
Asignar el puerto a una VLAN.	`S1(config-if)#switchport access vlan` *id de la VLAN*
Volver al modo EXEC privilegiado.	`S1(config-if)#end`

Tabla 5 Configuración de un puerto de acceso en un Switch [11]

3.4.7 Definición de enlace troncal de la VLAN

Un enlace troncal es un enlace punto a punto entre dos dispositivos de red que lleva más de una VLAN. Un enlace troncal de VLAN le permite extender las VLAN a través de toda una red.

Un enlace troncal de VLAN no pertenece a una VLAN específica, sino que es un conducto para las VLAN entre switches y routers.

La siguiente tabla muestra la configuración de un puerto troncal en un Switch.

Sintaxis del comando de la CLI del IOS de Cisco	
Ingresar el modo de configuración global.	`S1#configure terminal`
Ingresar el modo de configuración de interfaz para la interfaz definida.	`S1(config)#interface` *id de la interfaz*
Hacer que el enlace que conecta los switches sea un enlace troncal.	`S1(config-if)#switchport mode trunk`
Especificar otra VLAN como la VLAN nativa para los enlaces troncales IEEE 802.1Q sin etiquetar.	`S1(config-if)#switchport trunk native vlan` *id de la VLAN*
Volver al modo EXEC privilegiado.	`S1(config-if)#end`

Tabla 6 Configuración de un puerto troncal en un Switch [11]

3.5 Router CISCO modelo 2811

3.5.1 Router

El router es una computadora diseñada para fines especiales que desempeña un rol clave en el funcionamiento de cualquier red de datos. Los routers son responsables principalmente de la interconexión de redes por medio de:

- la determinación del mejor camino para enviar paquetes
- el reenvío de los paquetes a su destino

Un router conecta múltiples redes. Esto significa que tiene varias interfaces, cada una de las cuales pertenece a una red IP diferente. Cuando un router recibe un paquete IP en una interfaz, determina qué interfaz usar para reenviar el paquete hacia su destino. La interfaz que usa el router para reenviar el paquete puede ser la red del destino final del paquete (la red con la dirección IP de destino de este paquete), o puede ser una red conectada a otro router que se usa para llegar a la red de destino.

Generalmente, cada red a la que se conecta un router requiere una interfaz separada. Estas interfaces se usan para conectar una combinación de Redes de área local (LAN) y Redes de área extensa (WAN). Por lo general, las LAN son redes Ethernet que contienen dispositivos como PC, impresoras y servidores. Las WAN se usan para conectar redes a través de un área geográfica extensa. Por ejemplo, una conexión WAN comúnmente se usa para conectar una LAN a la red del Proveedor de servicios de Internet (ISP).

La tabla de enrutamiento del router se utiliza para encontrar la mejor coincidencia entre la dirección IP de destino de un paquete y una dirección de red en la tabla de enrutamiento. La tabla de enrutamiento determinará finalmente la interfaz de salida para reenviar el paquete y el router lo encapsulará en la trama de enlace de datos apropiada para dicha interfaz de salida [20].

3.5.2 Caracteristicas del Router 2811

Los routers Cisco 2811 admiten un módulo de red mejorado (NME) simple, cuatro tarjetas de interfaz WAN de alta velocidad simples o dos dobles (HWIC), dos AIM, dos módulos de datos de voz en paquete (PVDM), dos conexiones Fast Ethernet y 24 puertos de salida de alimentación telefónica IP, los cuales pueden ser instalados en el slot VIC (Voice Interface Card). [21]

3.5.3 Rutas estáticas

Las rutas estáticas se utilizan generalmente cuando se enruta desde una red a una red de conexión única. Una red de conexión única es una red a la que se accede por una sola ruta. Por ejemplo, observando la figura, vemos que cualquier red conectada a R1 sólo tendrá una manera de alcanzar otros destinos, ya sean redes conectadas a R2 o destinos más allá de R2. Por lo tanto, la red 172.16.3.0 es una red de conexión única y R1 es el router de conexión única.

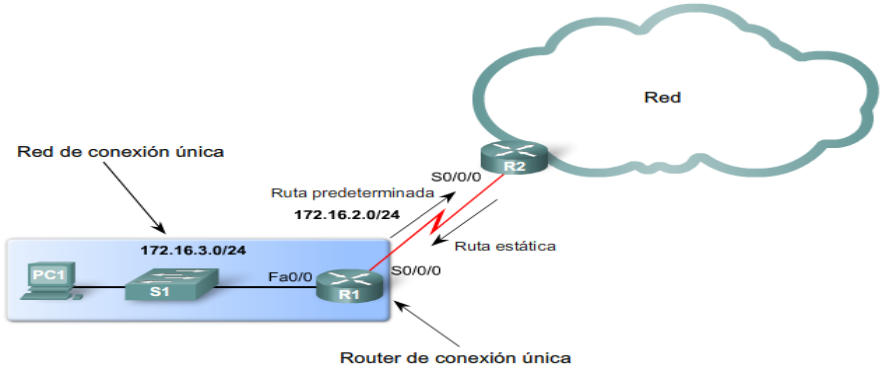


Figura 19 Ejemplo de una ruta estática

La ejecución de un protocolo de enrutamiento entre R1 y R2 es un desperdicio de recursos porque R1 sólo tiene una manera de enviar tráfico que no sea local. Por lo tanto, las rutas estáticas se configuran para obtener conectividad a redes remotas que no están conectadas directamente al router.

3.5.3.1 El comando ip route

El comando para configurar una ruta estática es ip route. La sintaxis para configurar una ruta estática es:

Router(config)#ip route network-address subnet-mask {ip-address | exit-interface }

Se utilizan los siguientes parámetros:

- network-address: dirección de red de destino de la red remota que se deberá agregar en la tabla de enrutamiento.
- subnet-mask: máscara de subred de la red remota que se deberá agregar en la tabla de enrutamiento. La máscara de subred puede modificarse para resumir un grupo de redes.

Además, deberá utilizarse uno de los siguientes parámetros o ambos:

- ip-address: generalmente denominada dirección IP del router de siguiente salto.
- exit-interface: interfaz de salida que se debería utilizar para reenviar paquetes a la red de destino.

3.5.4 Subinterfaces

Las subinterfaces son interfaces virtuales basadas en software asignadas a interfaces físicas. Cada subinterfaz se configura con su propia dirección IP, máscara de subred y asignación de VLAN única, lo que permite que una interfaz física única sea parte en forma

simultánea de múltiples redes lógicas. Esto resulta útil cuando se realiza el enrutamiento entre VLAN en redes con múltiples VLAN y pocas interfaces físicas del router.

Al configurar el enrutamiento entre VLAN, la interfaz física del router debe estar conectada al enlace troncal en el switch adyacente. Las subinterfaces se crean para cada VLAN/subred única en la red. A cada subinterfaz se le asigna una dirección IP específica a la subred de la cual será parte y se configura en tramas con etiqueta de la VLAN para la VLAN con la cual interactuará la interfaz. De esa manera, el router puede mantener separado el tráfico de cada subinterfaz a medida que atraviesa el enlace troncal hacia el switch [20].

3.5.4.1 Configuración de la subinterfaz

La sintaxis para la subinterfaz es siempre la interfaz física, por ejemplo f0/0, seguida de un punto y un número de subinterfaz. El número de la subinterfaz es configurable, pero generalmente está asociado para reflejar el número de VLAN. La interfaz física está especificada porque puede haber múltiples interfaces en el router, cada una configurada para admitir muchas subinterfaces.

Antes de asignar una dirección IP a una subinterfaz, es necesario configurar la subinterfaz para que funcione en una VLAN específica mediante el comando encapsulation dot1q id de la VLAN. Una vez asignada la VLAN, el comando ip address 192.168.10.1 255.255.255.0 asigna la subinterfaz a la dirección IP apropiada para esa VLAN.

Interfaz fisica	Subinterfaz
Una interfaz fisica por VLAN	Una interfaz física para muchas VLAN
No existe contención de ancho de banda	Contención de ancho de banda
Conectado para acceder al modo de puerto de Switch	Conectado para establecer el enlace troncal en el modo de puerto Switch
Más costoso	Menos costoso
Configuración de la conexión menos compleja	Configuración de la conexión más compleja

Tabla 7 Comparación de la interfaz del router y las subinterfaces

3.5.5 Listas de Acceso

La ACL es una configuración de router que controla si un router permite o deniega paquetes según el criterio encontrado en el encabezado del paquete. Las ACL también se utilizan para seleccionar los tipos de tráfico por analizar, reenviar o procesar de otras maneras.

Como cada paquete llega a través de una interfaz con una ACL asociada, la ACL se revisa de arriba a abajo, una línea a la vez, y se busca un patrón que coincida con el paquete

entrante. La ACL hace cumplir una o más políticas de seguridad corporativas al aplicar una regla de permiso o denegación para determinar el destino del paquete. Es posible configurar las ACL para controlar el acceso a una red o subred [22].

3.5.5.1 Características de las ACLs

Se pueden configurar las ACLs por protocolo, por dirección y por interfaz.

- Una ACL por protocolo: para controlar el flujo de tráfico de una interfaz, se debe definir una ACL para cada protocolo habilitado en la interfaz.
- Una ACL por dirección: las ACL controlan el tráfico en una dirección a la vez de una interfaz. Deben crearse dos ACL por separado para controlar el tráfico entrante y saliente.
- Una ACL por interfaz: las ACL controlan el tráfico para una interfaz, por ejemplo, Fast Ethernet 0/0.

3.5.5.2 Cómo funcionan las ACL

Las listas de acceso definen el conjunto de reglas que proporcionan control adicional para los paquetes que ingresan a las interfaces de entrada, paquetes que pasan a través del router y paquetes que salen de las interfaces de salida del router. Las ACL no actúan sobre paquetes que se originan en el mismo router.

Las ACL se configuran para ser aplicadas al tráfico entrante o saliente.

- ACL de entrada: los paquetes entrantes se procesan antes de ser enrutados a la interfaz de salida. Una ACL de entrada es eficaz porque guarda la carga de búsquedas de enrutamiento si el paquete se descarta. Si el paquete está autorizado por las pruebas, luego se procesa para el enrutamiento.
- ACL de salida: los paquetes entrantes se enrutan a la interfaz de salida y luego son procesados a través de la ACL de salida.

3.5.5.3 Tipos de ACLs

3.5.5.3.1 ACL estándar

Las ACL estándar le permiten autorizar o denegar el tráfico desde las direcciones IP de origen. No importan el destino del paquete ni los puertos involucrados. El ejemplo permite todo el tráfico desde la red 192.168.30.0/24. Debido a la sentencia implícita "deny any" (denegar todo) al final, todo el otro tráfico se bloquea con esta ACL. Las ACL estándar se crean en el modo de configuración global. [22]

Las ACLs estándar filtran paquetes IP solamente según la dirección de origen.

Ejemplo de configuración en el IOS CISCO

Access-list 10 permit 192.168.30.0 0.0.0.255

3.5.5.3.2 ACL extendidas

Las ACL extendidas filtran los paquetes IP en función de varios atributos, por ejemplo: tipo de protocolo, direcciones IP de origen, direcciones IP de destino, puertos TCP o UDP de origen, puertos TCP o UDP de destino e información opcional de tipo de protocolo para una mejor disparidad de control [22].

Las ACLs extendidas filtran paquetes según diferentes atributos, entre ellos los siguientes:

- Direcciones IP de origen y de destino
- Puertos TCP y UDP de origen y de destino
- Tipo de protocolo (IP, ICMP,UDP,TCP o número de protocolo)

Ejemplo de configuración en el IOS CISCO

Access-list 103 permit tcp 192.168.30.0 0.0.0.255 any eq 80

3.6 TelefoníaVoIP

3.6.1 Configuración del Gatekeeper SPA9000

El gatekeeper provee señalización, controla y enruta las llamadas por medio del protocolo SIP, lo que hace más eficiente el tránsito de tráfico de voz, ya que existe una ruta para éste y otra para la señalización.

Para poder acceder a la configuración, se conectó un cable Ethernet al puerto Ethernet WAN del SPA9000, conectando el otro extremo al puerto Ethernet de una computadora. La dirección IP por default del SPA9000 es 192.168.0.1 con máscara de red de 24 bits.

En el navegador web se escribe lo siguiente: 192.168.0.1/admin/voice/advancek, antes de ingresar la dirección, previamente se tiene que configurar una dirección IP en la computadora que será utilizada para administrar el SPA9000, esta dirección tiene que estar en el mismo segmento, es decir, cualquier dirección de 192.168.0.1 a 192.168.0.254, esto con el objeto de que la computadora y el SPA9000 se encuentren en la misma red local.

Una vez que ingresamos al SPA9000 por medio de la Web, saldrá la siguiente pantalla:

Figura 20 Pantalla inicial del SPA900

En la pestaña Router, seleccionamos Wan Setup y en esta se configura la IP y el Gateway, los cuales son 192.168.20.100 y 192.168.20.254 respectivamente. La dirección 192.168.20.100 se configuró por el diseño de la red, puesto que este Gateway de Voz esta en el Switch del Subscriptor en la VLAN 20.

Figura 21 Configuración de la dirección WAN

3.6.2 Configuración de los temporizadores

Para configurar los temporizadores utilizados por el protocolo SIP, se muestran en la siguiente tabla. Estos se encuentran estipulados y descritos en la RFC 3261.

Tipo de Temporizador	Valor	Descripción
T1	0.5 s	Cálculo de RTT (Round-trip Time)
T2	4 s	Intervalo máximo de retransmisión para peticiones no INVITE y para respuestas INVITE
T4	5 s	El período de tiempo máximo que un mensaje puede permanecer en la red
Temporizador B	$64 * T1$	Temporizador de tiempo de espera de transacciones INVITE
Temporizador D	> 32 segundos para UDP 0 segundos para TCP y SCTP	Tiempo de espera para retransmisiones de respuestas
Temporizador F	$64 * T1$	Temporizador de tiempo de espera de transacciones no INVITE
Temporizador H	$64 * T1$	Tiempo de espera para la recepción ACK
Temporizador J	$64 * T1$ para UDP 0 segundos para TCP y SCTP	Tiempo de espera para retransmisiones de peticiones no INVITE

Tabla 8 Valores predeterminados de los temporizadores del protocolo SIP [23].

Nota: INVITE Indica que el usuario o servicio está invitado a participar en una sesión.

3.6.3 Parámetros RTP

RTP transmite paquetes que contienen muestras de voz. Por lo cual es necesario configurar algunos parámetros de este para poder asegurar una buena calidad en las llamadas de voz.

Parámetro	Valor	Descripción
RTP Port Min	16384	Es el número de puerto mínimo para transmisiones yrecepciones RTP.
RTP Port Max	16482	Es el número de puerto máximo para transmisiones yrecepciones RTP.
RTP Packet Size	0.030	Se refiere al tamaño aproximado del paquete de voz RTP ensegundos. Puede ser desde 0.01 a 0.16 s, los valoresutilizados sólo pueden ser múltiplos de 0.01. El tamaño quese utilizó fue de 0.030 s, debido a qué es un valortípicamente usado por los códecs que maneja el SPA9000.

Tabla 9 Valores predeterminados de los parámetros RTP [23]

La configuración de estos distintos valores se muestra a continuación.

Figura 22 Configuración de los temporizadores SIP y parámetros RTP

3.6.4 Configuración de los teléfonos IP Linksys

Los teléfonos IP Linksys utilizados son los modelos SPA922 y SPA94. Los teléfonos Linksys se registran automáticamente en el SPA9000, aunque su dirección IP y su extensión se configuran en el teléfono.

La configuración de los teléfonos se realizó a través de Web Browser al igual que el SPA9000.

Para poder acceder via web a la administración de los teléfonos, necesitamos conocer la IP que tiene configurada actualmente el teléfono, para poder verificar dicha dirección IP, realizamos lo siguiente:

1.- El teléfono cuenta con un botón de administración, una vez que accedemos al menu, seleccionamos la opcion de network, la cual muestra distintos parametros, entre los cuales se encuentra, la direccion IP, la mascara de red, el Default Gateway, entre otros parametros.

2.- Una vez que conocemos la direccion IP del telefono, la ingresamos en el navegador web, previamente conectamos mediante un cable Ethernet nuestra computadora y el telefono asignando una direccion IP del mismo segmento del telefono a la computadora, con el objeto de que se encuentren en la misma red local y estos puedan tener comunicación.

3.- Una vez dentro de la aplicación, seleccionamos la pestaña System y procedemos a configurar la direccion IP, la mascara de red y el Gateway.

La direccion IP asigana fue: 192.168.2.11 la cual esta en el segmento del Switch de la BS en la VLAN 2.

La máscara de red asignada fue de 24 bits, es decir, 255.255.255.0

El Gateway configurado fue el 192.168.2.254

La siguiente figura muestra la configuracion.

Figura 23 Configuración del teléfono IP Linksys

La configuración de los temporizadores SIP y de los parámetros RTP fueron los mismos que se configuraron en el SPA9000.

Figura 24 Configuración de los temporizadores SIP y de los parámetros RTP

Para configurar la extensión telefónica así como el nombre, se selecciona la pestaña Phone y la pestaña EXT 1, en estas dos se configuran dichos parámetros.

Figura 25 Configuración del nombre del dispositivo

La siguiente figura, muestra la configuración del número de extensión.

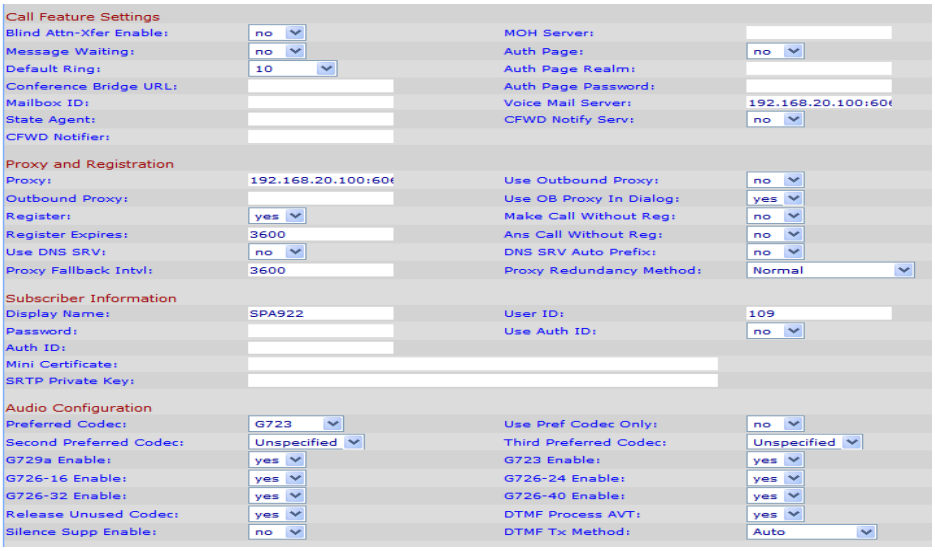


Figura 26 Configuración del número de extensión

La configuración anteriormente mostrada se realizó para el modelo SPA922, la configuración para el modelo SOA941 es la misma.

CAPITULO IV

QoS y Aplicaciones de red

Una red basada en la conmutación de paquetes sufre de fenómenos particulares que dificultan el traslado de los paquetes. Las causas de dichos fenómenos se deben principalmente a la congestión de la red, es decir a transmitir datos a una velocidad mayor a la que el canal es capaz de transmitir.

Al emplear servicios de voz, video y datos se espera que la infraestructura de la red llegué a su límite y con ello se degrada la calidad de los servicios. Los fenómenos antes mencionados así como su afectación a los servicios se exponen en este capítulo. Posteriormente se ejemplifica cómo la QoS de CISCO mitiga estos sucesos.

Finalmente se explica la configuración de los servicios de video-streaming y transferencia de datos (FTP).

4.1 Calidad de servicio QoS

Actualmente las redes soportan diferentes tipos de aplicaciones tales como voz, vídeo y datos sobre una infraestructura común. La convergencia de todos estos tipos de aplicaciones conjuntas representa un reto para el personal administrador encargado de ello.

El retardo aceptable para un paquete de VoIP es de 150 a 200 ms y el jittero variación en el retardo ha de ser mínimo para mantener la consistencia de la llamada. Por el contrario, una aplicación de datos tal como FTP no es tan sensitiva al retardo y el jitter ni siquiera sería apreciado. Cuando conjuntamente existen voz y datos en la red se deben usar mecanismos para hacer que puedan coexistir.

Muchas aplicaciones de datos están basadas en protocolos orientados a la conexión como TCP, cuando pierden un segmento otro es retransmitido, mientras que las aplicaciones de voz o vídeo tienen una tolerancia mínima hacia las pérdidas de datos. Debido a esto es necesario implementar mecanismos que prioricen determinados tipos de tráfico cuando exista congestión en la red.

Los fallos en la red afectan a todas las aplicaciones, mientras la red converge después de un fallo quienes más sufren el desperfecto son los usuarios que estén usando aplicaciones interactivas de voz o vídeo, pudiendo incluso perder la llamada [24].

Existen cuatro cuestiones importantes a tener en cuenta en redes convergentes:

- Ancho de banda disponible
- Retraso de extremo a extremo
- Jitter o fluctuaciones en el retraso
- Pérdidas de paquetes

4.1.1 Ancho de banda disponible

El ancho de banda disponible es el máximo ancho de banda de la ruta dividido entre el número de flujos.

La falta de ancho de banda hace que las aplicaciones se degraden debido al retraso y a la pérdida de paquetes. Esto es detectado de forma inmediata por los usuarios de aplicaciones de voz o vídeo.

Es posible resolver los problemas de ancho de banda con algunos de los siguientes recursos:

- Incrementar el ancho de banda. Lo cual es efectivo pero costoso. Aunque dependiendo del escenario en algunos casos es recomendable.
- Usar mecanismos de QoS de clasificación y marcado así como mecanismos de encolamiento apropiados. De esta manera se enviarán primero los paquetes más importantes.

- Usar técnicas de compresión. Compresión a capa 2, compresión de cabeceras TCP, cRTP (RTP header compression), etc. Siempre es preferible compresión en hardware en vez de en software, ya que el mecanismo en sí usa muchos recursos de CPU.

4.1.2 Retraso de extremo a extremo

Hay diferentes tipos de retraso desde origen a destino. El retraso de extremo a extremo es la suma de estos cuatro tipos de retraso:

- Retraso de procesamiento, es el tiempo que un dispositivo de capa 3 tarda en mover un paquete desde la interfaz de entrada a la de salida. El tipo de CPU así como la arquitectura de hardware influyen en esto.
- Retraso de encolamiento, es el tiempo que un paquete pasa en la cola de salida de una interfaz. Dependerá de lo ocupado que esté el router, del número de paquetes esperando, del tipo de cola y del ancho de banda de la interfaz.
- Retraso de señalización, es el tiempo empleado en poner en el medio físico todos los bits de una trama.
- Retraso de propagación, es el tiempo que se tarda en transmitir en el medio físico los bits correspondientes a una trama. Depende del tipo

4.1.3 Variación del retraso

Las fluctuaciones en el retraso reciben el nombre de Jitter. Se producecuando los paquetes llegan al destino a velocidades diferentes a las que se emitieron desde el origen. Para paquetes de VoIPo vídeo es esencial que laaplicación sea capaz de liberarlos en el destino a la misma velocidad y en el mismo orden que fueron emitidos en un principio. Esto lo hace sirviéndose del buffer, que es donde se van almacenando a medida que llegan y de RTP(Real-Time TransportProtocol) que sella los paquetes para que sean entregados en orden [24].

Algunas de las claves para ayudar a reducir el jitter son las siguientes-

- Incrementar en ancho de banda.
- Priorizar los paquetes sensitivos.
- Usar técnicas de compresión de capa 2.
- Usar técnicas de compresión de cabeceras.

4.1.4 Pérdida de paquetes

La pérdida de paquetes ocurre cuando un router no tiene más espacio libre en el buffer de memoria de la interfaz de salida para almacenar los nuevos paquetes que le llegan, debiendo descartarlos.

TCP reenvía los paquetes descartados, a la vez que reduce el tamaño de ventana. Aplicaciones UDP como TFTP por ejemplo pueden generar más tráfico la red al tener que retransmitir un archivo completo en caso de pérdida de paqueh Para llamadas de VoIP la pérdida de paquetes resulta en conversaciones entrecortadas, mientras que para vídeo la imagen parece congelarse. Con los mecanismos de QoS adecuados es posible evitar estas situaciones [24].

- A través del comando show interface es posible información cuando existan pérdidas de paquetes o congestión.
- Output drop: número de paquetes descartados, debido cola de salida de la interfaz está llena.
- Input queue drop: si la CPU está sobrecargada el router podría tener problemas al procesar paquetes entrantes, incrementándose este contador.
- Ignore: número de tramas ignoradas debido a falta de espacio en el buffer.
- Overrun: cuando la CPU está sobrecargada podría no proporcionar espacio en el buffer lo suficientemente rápido, haciendo que se descarten paquetes.
- Frame error:incluye las tramas con CRC (Cyclic Redundancy Check) no válido, las que son más pequeñas que el standard (runts) y las gigantes (giants).

Los siguientes métodos pueden utilizarse para reducir o evitar la pérdida de paquetes:

- Incrementar el ancho de banda.
- Incrementar el tamaño del buffer. Modificando los valores por defecto.
- Proporcionar un ancho de banda garantizado. Usando herramientas de QoS tales como CBWFQ (Class Based Weighted Fair Queuing) o LLQ (Low Latency Queuing).
- Evitar la congestión. Descartando aleatoriamente paquetes antes de que las colas se llenen. Para esto existen métodos como RED(Random Early Detection) y WRED(Weighted Random Early Detection).

4.1.5 Implementación de QoS

QoS se define como la habilidad de la red para proporcionar un mejor o especial servicio a un conjunto de usuarios o aplicaciones en detrimento de otros usuarios o aplicaciones.

Para implementar QoS hay que llevar a cabo tres pasos:

- Identificar tipos de tráfico y sus requerimientos.
- Clasificación del tráfico basándose en los requerimientos identificados.
- Definir las políticas para cada clase.

4.1.5.1 Identificación del tráfico y sus requerimientos

Es el punto de partida en cualquier implementación de QoS y conlleva los siguientes apartados:

- Llevar a cabo una auditoria de red. Es aconsejable tomar estos datos durante los momentos en que la red esté más ocupada así como durante otros periodos.
- Determinar la importancia de cada aplicación. El modelo de negocio determinará la importancia de cada aplicación. Se pueden definir clases de tráfico y los requerimientos para cada clase.
- Definir niveles de servicio para cada clase de tráfico. Cada clase identificada previamente ha de tener un nivel de servicio que constará de características como ancho de banda garantizado, retraso, preferencia a la hora de que se descarte. Etc.

4.1.5.2 Definición de políticas para cada clase

Este paso conlleva el completar las siguientes tareas:

- Especificar un ancho de banda máximo.
- Especificar un ancho de banda mínimo garantizado.
- Asignar niveles de prioridad.
- Usar herramientas que sean adecuadas para la congestión gestionándola, eliminándola, etc.

La tabla siguiente muestra un ejemplo de una política de QoS.

Clase	Prioridad	Tipo de cola	Ancho de banda Min/Max	Herramienta
Voice	5	Prioridad	1 Mbps Min 1 Mbps Max	Prioridad de cola
Business mission critical	4	CBWFQ	1 Mbps Min	CBWFQ
SSignaling	3	CBWFQ	400 Kbps Min	CBWFQ
Transactional	2	CBWFQ	1 Mbps Min	CBWFQ
Best-effort	1	CBWFQ	500 Kbps Max	CBWFQ CB-Policing
Scavenger	0	CBWFQ	Max 100 Kbps	CBWFQ CB-Policing WRED

Tabla 10 Políticas de QoS [24]

4.1.6 Modelo de QoS

Modelo Best-Effort

El modelo Best-Effort significa que no hay QoS aplicado, de manera que todos los paquetes dentro de la red independientemente del tipo que sean reciben el mismo trato. Como beneficio de este sistema está la facilidad de implementación, ya que no hay que hacer nada para ponerlo en funcionamiento, pero tiene como desventaja que no es posible garantizar ningún tipo de servicio a ninguna aplicación.

4.1.6.1 Modelo de servicios integrados

Se trata del primer modelo que proporcionó QoS de extremo a extremo y basado en la señalización explícita y reserva de recursos de red para aquellas aplicaciones que los necesitan. El protocolo usado para la señalización es el RSVP(Resource Reservation Protocol). Cuando una aplicación tiene un requerimiento de ancho de banda RSVP va salto por salto a lo largo del camino intentándola hacer la reserva solicitada en cada uno de los routers que se encuentra en la ruta. Si la reserva se puede hacer la aplicación podrá operar; pero si algún elemento *en el* camino no tiene los recursos suficientes la aplicación tendrá que esperar.

Para implementar Servicios Integrados de manera satisfactoria además de RSVP debería habilitarse lo siguiente:

- Control de Admisión, en caso de que los recursos no puedan proporcionarse sin afectar a las aplicaciones actualmente en uso se deberían denegar.

- Clasificación, el tráfico perteneciente a una aplicación que ha solicitado una reserva se debería clasificar y ser reconocido por los routers en el camino.
- Políticas, es necesario tomar acciones cuando las aplicaciones excedan la utilización de los recursos acordados.
- Encolamiento, es importante que los dispositivos almacenar los paquetes mientras se envían los que primero.
- Programación, funciona junto con el encolamiento y hacereferencia al caso en el que existan varias colas y qué cantidad de datos podrían transmitir cada una en cada ciclo.

Los beneficios de Servicios Integrados son el control de admisión de recursos de extremo a extremo, políticas de control de admisión por petición y señalización de números de puerto dinámicos. Como desventajas mencionar que cada flujo activo necesita señalización continua, usando así recursos extra y haciendo que no sea un modelo altamente escalable [24].

4.1.6.2 Modelo de servicios diferenciados

Éste modelo es el más actual de los tres y ha sido desarrollado para suplir las deficiencias de sus predecesores. Está explicado detalladamente en las RFC 2474 y 2475.

Servicios Diferenciados usa PHB (Per-Hop Behavior), que hace referencia al comportamiento por salto. Esto significa que cada salto en el camino está programado para proporcionar un nivel de servicio específico a cada clase de tráfico.

Con este modelo, el tráfico es en principio clasificado y marcado. Amedida que fluye en la red va recibiendo distinto trato dependiendo de su marca.

En los servicios diferenciados hay que tener en cuenta que:

- El tráfico es clasificado.
- Las políticas de QoS son aplicadas dependiendo de la clase.
- Se debe elegir el nivel de servicio para cada tipo de clase que corresponderá a unas necesidades determinadas.

Como ventajas principales mencionar la escalabilidad y habilidad para soportar muchos tipos de niveles de servicio. Como puntos negativos el servicio no es absolutamente garantizado y es más complejo de implementar.

4.1.7 Implementación de QoS

Interfaz de línea de comandos de QoS modular

Cisco ha introducido MQC (Modular QoS Command-Line Interface) para las limitaciones del método anterior, además de incluir la utilización de nuevas herramientas de QoS. Se trata de una arquitectura modular y eficiente.

Implementar QoS con MQC requiere de tres pasos necesarios:

Definir las clases de servicio usando el comando class-map

Definir políticas para las clases definidas usando policy-map.

Aplicar las políticas en dirección de entrada o salida a una interfaz, usando el comando service-policy.

A cada class map se le aplica un nombre, sensitivo a mayúsculas, minúsculas, y está compuesta por una o más sentencias. Una o todas esas sentencias deben coincidir dependiendo de si el class map tiene el parámetro match-any o match-all, y en caso de no estar definido por defecto está match-all.

El ejemplo que sigue muestra dos class maps. La primera se llama VoIP y especifica que todo el tráfico que pase por la ACL 100 será clasificaso como VoIP. La segunda es llamada Videoconferencia y especifica que todo el tráfico que pase por la ACL 101 será clasificado como aplicaciones de la empresa [24].

class-map VoIP
match access-group 100
!
class-mapVideoconferenciamatch access-group 101

En el ejemplo ambos class map tienen una sola sentencia y como no se ha especificado match-any o match-all aplica el de por defecto que es match-all, aunque al tener una sola sentencia el resultado sería el mismo independientemente de cuál se aplique. También se podría utilizar la condición no match.

En la siguiente sintaxis se asocian las características de QoS requeridas a cada clase. Un policy map tiene un nombre sensitivo a mayúsculas y minúsculas y permite tener asociadas hasta 256 clases. Se observa como la clase VoIP es asignada a una cola de prioridad estricta con un ancho de banda garantizado de 256 Kbs. La clase Videoconferenciaha sido asignada a una cola WFQ en la que contará con un mínimo de

ancho de banda de 256 Kbs. Todo el tráfico restante será asignado a la clase class-default y le será dado el ancho de banda restante.

policy-map Politicas
class VoIP
priority 256
class Videoconferencia
bandwidth 256
class class-default
fair-queue

Finalmente se aplica el policy map a una interfaz, pudiendo aplicarlo a más de una, y dependiendo de la configuración será de entrada o salida. En el ejemplo siguiente se aplica a la interfaz serial 1/0 en dirección de salida:

Interface serial 1/0
Service-policy output Politicas

Los siguientes tres comandos ayudan a mostrar y verificar las clases y políticas configuradas así como las aplicadas a una interfaz:

- show class-map
- show policy-map
- show policy-map interface interface

4.1.7.1 (Differentiated Service Code Point) (DSCP)

Los seis bits más significativos del campo DiffServ son conocidos como DSCP. Los dos últimos bits en el campo DiffServ no se han definido dentro de la arquitectura de campo DiffServ, los cuales ahora se utilizan como una notificación explícita de congestión de bits. Los routers en el borde de la red se encargan de clasificar los paquetes y marcarlos, ya sea con la IP o DSCP como valor en una red Diffserv. Los dispositivos de red de capa 3 con el apoyo de Diffserv utiliza el valor de DSCP en el encabezado IP para seleccionar un comportamiento PHB para el paquete y proporcionar el tratamiento adecuado de calidad de servicio. [25]

P2	**P1**	**P0**	**T2**	**T1**	**T0**	**CU1**	**0 um**

- IP de prioridad, tres bits (P2 a P0)

- Delay, rendimiento y fiabilidad tres bits (T2 a T0)
- CU (Actualmente no se usa) y dos bits (CU1-0 um)

DiffServ campo

DS5	**DS4**	**DS3**	**DS2**	**DS1**	**DS0**	**ECN**	**ECN**

- DSCP seis bits (DS5-DS0)
- ECN-dos bits

El campo DiffServ estandarizado del paquete se marca con un valor de modo que el paquete recibe un tratamiento particular o de reenvío de PHB, en cada nodo de la red

El valor por defecto es 000 000 DSCP. Clase DSCPs selectores son los valores que son compatibles con la prioridad de IP. Cuando la conversión entre la prioridad de IP y DSCP, coinciden con los tres bits más significativos. En otras palabras:

IP prec **cinco** (101) asigna a IP DSCP **101 000**

Términos de Byte

1	**0**	**1**	**T2**	**T1**	**T0**	**UM2**	**0 um**

DiffServ campo

1	**0**	**1**	**0**	**0**	**0**	**ECN**	**ECN**

El estándar DiffServ utiliza los mismos bits de prioridad (los más significativos son los bits DS5, DS4 y DS3) para el establecimiento de prioridades, en donde se ofrece una inspección más fina a través del uso de los siguientes tres bits en el DSCP. DiffServ reorganiza y cambia el nombre de los niveles de prioridad (aún definido por los tres bits más significativos de la DSCP) en estas categorías [25].

Nivel de Prioridad	Descripción
7	Sigue siendo la misma (capa de enlace de protocolo de enrutamiento y de mantener vivo)
6	Sigue siendo el mismo (para protocolos de enrutamiento IP)
5	Express Forwarding (EF)
4	Clase 4
3	Clase 3
2	Clase 2
1	Clase 1
0	Mejor esfuerzo

Tabla 11 Niveles de prioridad [25]

Con este sistema, un dispositivo prioriza el tráfico por la primera clase. A continuación, se diferencia y da prioridad a la misma clase de tráfico, teniendo la probabilidad de que el tráfico caiga.

El estándar DiffServ no especifica una definición precisa de "baja", "medio" y "alta" referente a la probabilidad de descarte. No todos los dispositivos reconocen la configuración de los DiffServ (DS2 y DS1), e incluso cuando estos valores son reconocidos, no necesariamente desencadenan la misma acción de PHB de reenvío en cada nodo de la red. Cada nodo ejecuta su propia respuesta en función de cómo esté configurado.

4.1.7.2 Assured Forwarding

RFC 2597 define el reenvío asegurado (AF) PHB y lo describe como un medio para un dominio de proveedor de DS para ofrecer diferentes niveles de garantías para el reenvío de paquetes IP recibidos de un cliente de dominio DS. El Assured Forwarding PHB garantiza una cierta cantidad de ancho de banda a una clase de AF y permite el acceso a ancho de banda adicional, si está disponible. Hay cuatro clases de AF, a través AF1x AF4x. Dentro de cada clase, hay tres probabilidades de caída. Dependiendo de la política de una red dada, los paquetes pueden ser seleccionados para un PHB basada en el rendimiento requerido, retardo, jitter, pérdida o de acuerdo a la prioridad de acceso a los servicios de red.

Las clases 1 a 4 se refieren como clases de AF. La siguiente tabla muestra la codificación DSCP para especificar la clase de enfoque automático con la probabilidad. Bits DS5, DS4 y DS3 definir la clase, los bits y DS1 DS2 especificar la probabilidad de caída; DS0 bit es siempre cero [26].

Nivel	Clase 1	Clase 2	Clase 3	Clase 4
Bajo	001010	010010	011010	100010
	AF11	AF21	AF31	AF41
	DSCP 10	DSCP 18	DSCP 26	DSCP 34
Medio	001100	010100	011100	100100
	AF12	AF 22	AF32	AF42
	DSCP 12	DSCP 20	DSCP 28	DSCP 36
Alto	001110	010110	011110	100110
	AF13	AF23	AF33	AF43
	DSCP 14	DSCP 22	DSCP 30	DSCP 38

Tabla 12 Valores de DSCP asociados a cada clase [25]

111110	**Reservado (routing y contol)**	**011110**	**Assured Clase 3 Preced. Alta**
111100	Reservado (routing y contol)	011100	Assured Clase 3 Preced. Media
111010	Reservado (routing y contol)	011010	Assured Clase 3 Preced. Baja
111000	Reservado (routing y contol)	011000	Configurable por el usuario
110110	Reservado (routing y contol)	010110	Assured Clase 2 Preced. Alta
110100	Reservado (routing y contol)	010100	Assured Clase 2 Preced. Media
110010	Reservado (routing y contol)	010010	Assured Clase 2 Preced. Baja
110000	Reservado (routing y contol)	010000	Configurable por el usuario
101110	Expedited (Premium)	001110	Assured Clase 1 Preced. Alta
101100	Configurable por el usuario	001100	Assured Clase 1 Preced. Media
101010	Configurable por el usuario	001010	Assured Clase 1 Preced. Baja
101000	Configurable por el usuario	001000	Configurable por el usuario
100110	Assured Clase 4 Preced. Alta	000110	Configurable por el usuario
100100	Assured Clase 4 Preced. Media	000100	Configurable por el usuario
100010	Assured Clase 4 Preced. Baja	000010	Configurable por el usuario
100000	Configurable por el usuario	000000	Besr Effort (Default)

Tabla 13 Valores estandarizados para DSCP [25]

4.1.7.3 Expedited Forwarding

RFC 2598 define el reenvío acelerado (EF) PHB: "El EF PHB puede ser utilizado para construir una baja pérdida, baja latencia, el jitter bajo, ancho de banda de la seguridad de extremo a extremo de servicio a través de DS (Diffserv), un servicio de dominios aparece. a los extremos, como una conexión punto a punto o una "línea virtual alquilada." Este servicio también ha sido descrito como un servicio de primera calidad. " Codepoint 101110 se recomienda para el PHB EF, que corresponde a un valor DSCP de 46. [27]

Una vez más, el vendedor los mecanismos específicos que ser configurado para implementar estas empresas del sector privado. Consulte RFC 2598 para obtener más información acerca de EF PHB.

4.2 VLC Media Player

Para comenzar este es un programa de licencia gratuita y código abierto, tiene las capacidades de reproducir contenido multimedia, transcodificar, fungir como servidor de streaming a redes tanto locales como remotas a través de varios protocolos cómo FTTP, RTP, UDP y también puede actuar cómo cliente de streaming. Además cuenta con el respaldo de una gran comunidad que resulta útil para el uso de las funciones avanzadas.[9]

El proceso para implementar el streaming de video a redes remotas [9] requiere que el video sea convertido a un formato que resista la transmisión, este puede realizarse antes de la transmisión o al mismo tiempo. La computadora utilizada para transmitir no soportó la segunda opción por lo que primero convertimos el video en su totalidad a través de lasiguiente interfaz gráfica seleccionando medio/convertir:

Figura 27 Interfaz gráfica de VLC

Lo anterior abre una ventana para indicar el video origen, el destino y el formato tanto de transcodificación (H264 o MPEG-AVC) cómo el del contenedor (MPEG TS):

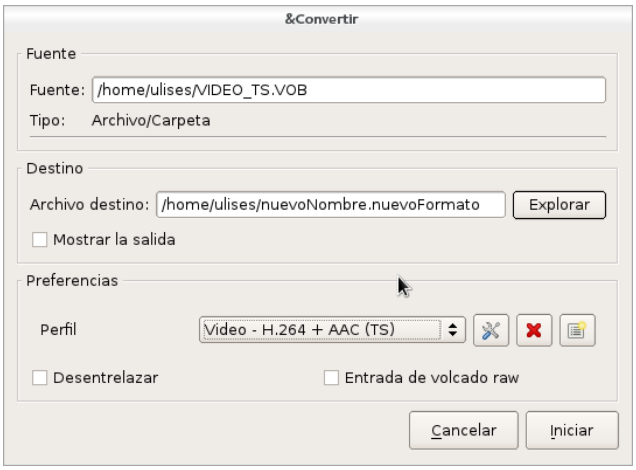


Figura 28 Menú “Convertir”

Para realizar el streaming a redes remotas se elige la opción medio/emitir, a lo que el programa desplegará la siguiente ventana:

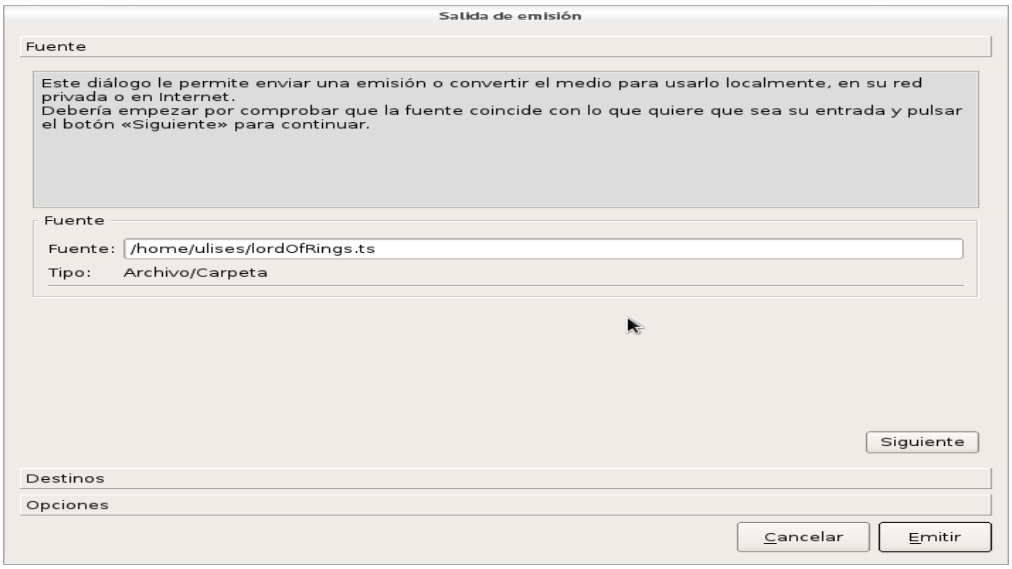


Figura 29 Menú principal de emisión

En dicha ventana se comienza por la selección del video a transmitir, en seguida se elige el protocolo de transporte que en nuestro caso es RTP para MPEG-TS, es importante deshabilitar la transcodificación ya que realizamos esto anteriormente y el video ya se encuentra en el formato deseado.

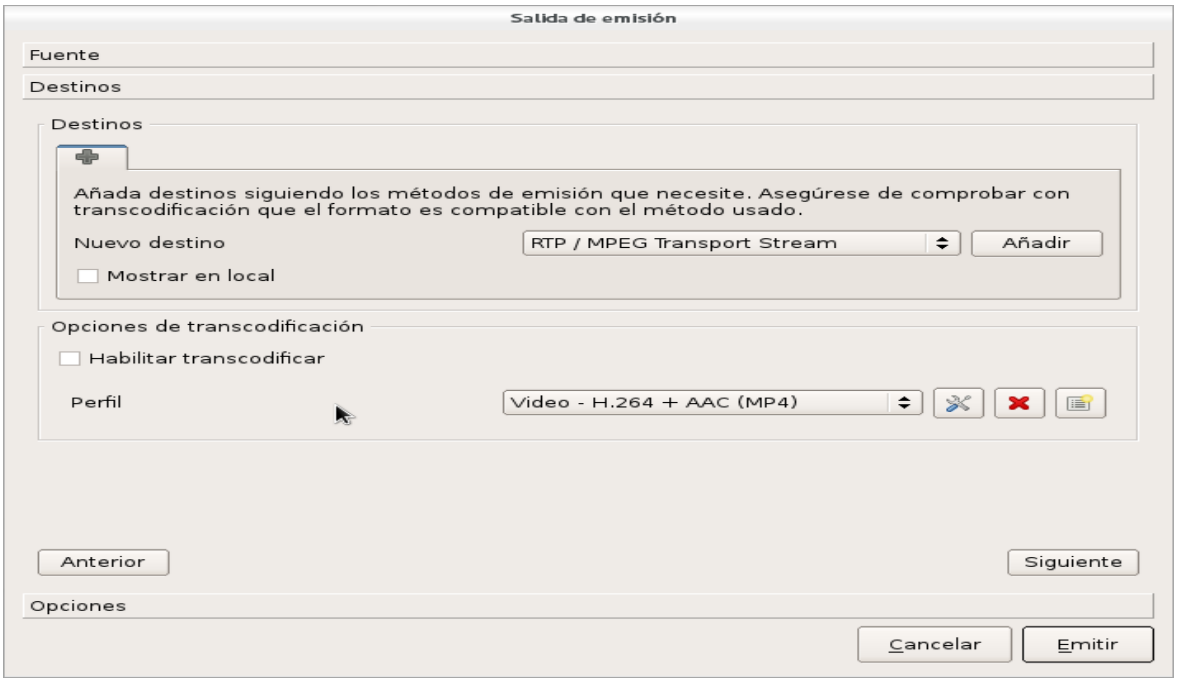


Figura 30 Menú “Protocolo de envío”

La opción mostrar permite observar desde la computadora en modo servidor lo que se está transmitiendo, esto resulta útil para comparar la degradación en la calidad del video.

Al seleccionar el protocolo de transporte se abre una opción para indicar la dirección ip del dispositivo la que será enviada la transmisión:

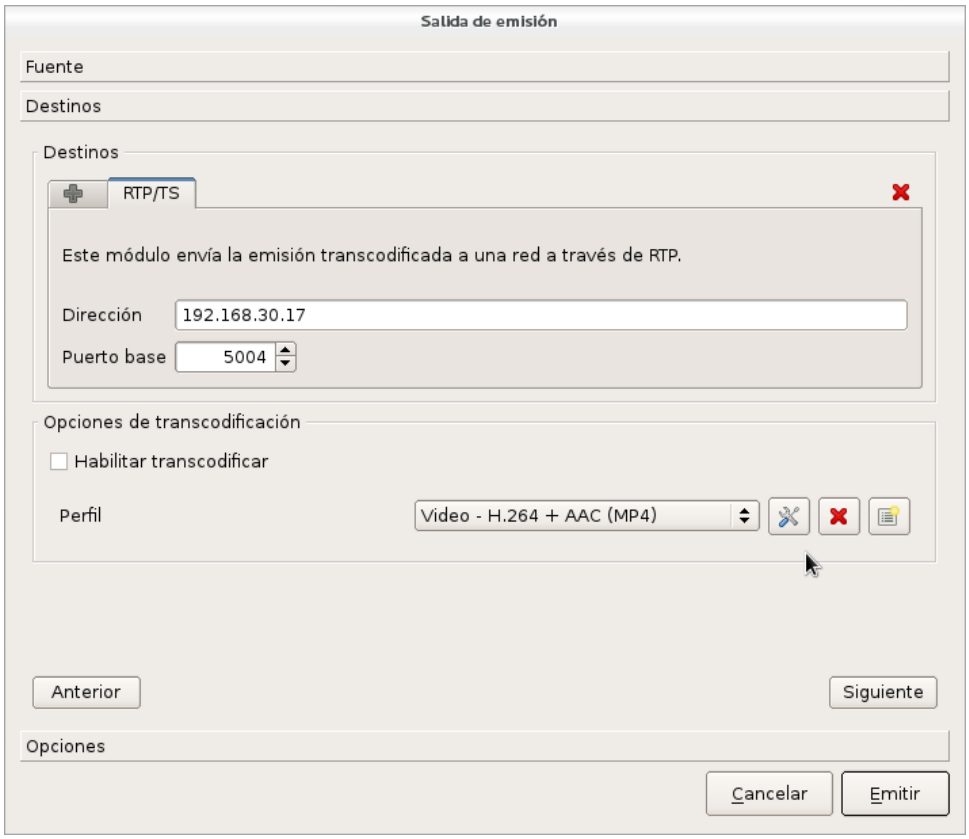


Figura 31 Menú “Destinos”

Finalmente se abre una nueva ventana donde aparece el comando equivalente a lo que se está solicitando hacer a VLC, además aparecen las últimas opciones a activar en la transmisión, de ellas la única relevante es el valor de TTL puesto que por cada router que atraviesa el flujo de video el TTL del paquete decrece una unidad y de volverse cero el paquete es descartado.

Cómo en la red ocupamos dos routers el TTL debe de establecerse al menos en 3:

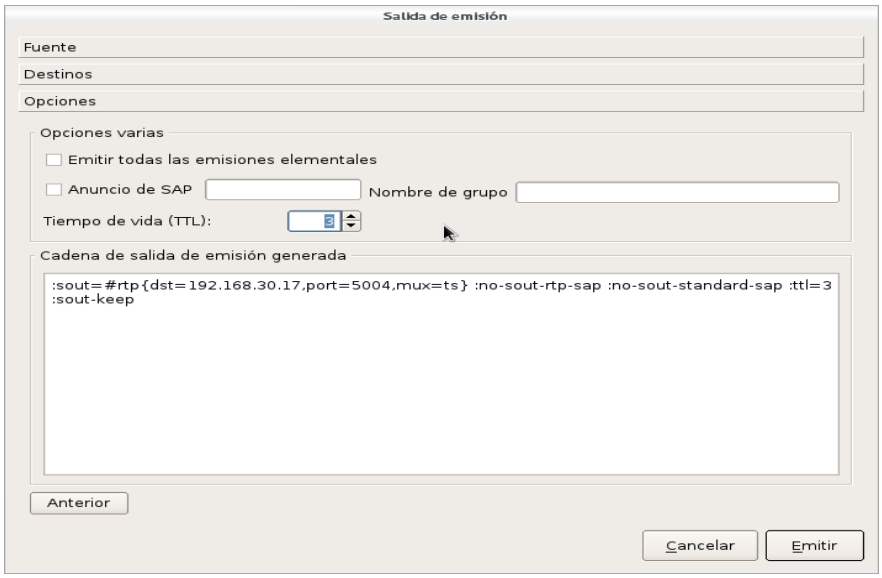


Figura 32 Opciones de red

Para comenzar la reproducción en el lado del cliente también se abre la interfaz gráfica de VLC, se elige la opción medio/Abrir volcado de red lo cual despliega la siguiente ventana, para comenzar a reproducir se indica en la casilla el protocolo de transporte seguido del puerto y finalmente se da click en reproducir.

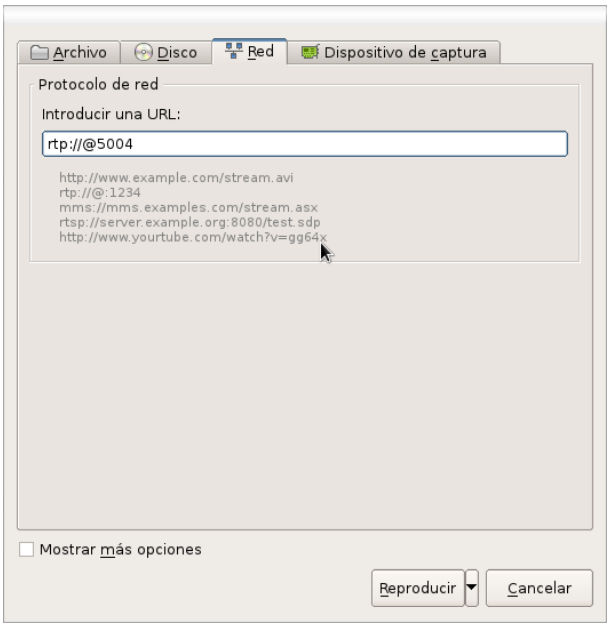


Figura 33 Reproducción de video en el cliente

4.3 VSFTPD

VSFTPD es un servidor de FTP nativo de linux, se configura y opera desde línea de comandos (shell); [28]Sin embargo se encuentra preconfigurado así que para poder utilizarlo sólo hace falta editar los valores de las siguientes variables en el archivo vsftpd.conf, el proceso en general para activar y utilizar el servidor es el siguiente:

Instalar el servidor: Las distribuciones más recientes de linux cuentan con gestores de instalación tanto gráficos cómo desde la línea de comandos, en nuestro caso usamos el sistema operativo fedora 16 por lo que la instalación a través del gestor se ejecutó con el siguiente comando:

```
#yum install -y vsftpd
```

Se edita el archivo vsftpd.conf para permitir la identificación mediante las cuentas de usuario del equipo (servidor) y activamos el usuario anomymus.

```
#vi /etc/vsftpd/vsftpd.conf
listen=YES
anonymus_enable=YES
local_enable=YES
```

Se copian los archivos a descargar mediante el comando:

```
#cp archivo_origen /var/ftp/nombreNuevo
```

Por último se activa el servidor con el comando:

```
#service vsftpd start
```

Desde el equipo del cliente (puede ser cualquier sistema operativo) se ejecutan los siguientes comandos para descargar los archivos:

```
carpeta_actual> ftp ip_servidor
user:
password:
ftp>get nombreArchivo
```

4.4 iPERF

iPERF es una herramienta con la capacidad de inyectar tráfico TCP ó UDP de extremo a extremo de una red y repotar las características de dicho flujo, se emplea mediante linea de comandos y puede especificarse el tipo de tráfico deseado mediante las siguientes banderas:

-s	configura la PC como le servidor de tráfico
-c	configura la PC como el cliente de tráfico
-d	establece el flujo de datos como bidireccional
-l	longitud del buffer de lectura/escritura
-w	tamaño de la ventana TCP
-i	intervalo de tiempo entre reportes
-t	intervalo de tiempo de la simulación total
-P	número de clientes paralelos a simular
-f	formato, reporte en kbps, mbps, Kbps, Mbps

Tabla 14 Banderas del comando iPERF [29]

Hay que destacar que operando bajo la inyección de tráfico tcp iPERF se adpta al canal de tal manera que transmite a la máxima velocidad de transmisión que le permita el enlace.
En sistemas windows no es necesario instalar el programa, sólo se descarga el ejecutable, luego se ingresa al cmd y entra a la dirección de este, finalmente sólo se ingresa el comando requerido. [29]

4.5 nTop

NTOP (Network TOP) permite monitorizar en tiempo real los usuarios y aplicaciones que están consumiendo recursos de red en un instante concreto. Posee un microservidor web que permite que cualquier usuario, que sepa la clave, pueda ver la salida NTOP de forma remota con cualquier navegador, y además es GNU. El software esta desarrollado para platarfomas Unix y Windows.

En Modo Web, actúa como un servidor de Web, volcando en HTML el estado de la red. Viene con un recolector/emisor NetFlow/sFlow, una interfaz de cliente basada en HTTP para crear aplicaciones de monitoreo centradas en top, y RRD para almacenar persistentemente estadísticas de tráfico.

Los protocolos que es capaz de monitorizar son: TCP/UDP/ICMP, (R)ARP, IPX, DLC, Decnet, AppleTalk, Netbios, y ya dentro de TCP/UDP es capaz de agruparlos por FTP, HTTP, DNS, Telnet, SMTP/POP/IMAP, SNMP, NFS, X11. [30]

La instalación en un sistema linux es la siguiente:

1) Se ingresa a una terminal del sistema.
2) Se ejecuta el gestor de paquetes solicitando la instalación de ntop, para fedora es el siguiente comando:

yum install -y ntop

3) se activa el servicio mediante el comando:

ntop -i nombreInterfazMonitoreo

4) Se ingresa al navegador web la dirección 127.0.0.1 y desde allí se pueden ver las estadísticas del tráfico.

CAPITULO V

Red

En este capítulo se describe cómo fueron realizadas las conexiones físicas y lógicas entres las computadoras clientes y/o servidores y los distintos dispositivos de red. Las conexiones físicas se refieren al cableado entre las distintas interfaces de red y las lógicas a direccionamiento IP implementado.

Además se reportan las configuraciones de QoS empleadas y cómo fueron usadas para cada caso en particular.

5.1 Estructura

Usamos dos grupos de equipos CISCO interconectados mediante un enlace WiMAX, cada grupo compuesto por un switch y un router. En el switch los puertos se asignan a tres VLAN diferentes para simular redes dedicadas al servicio de voz, video y datos respectivamente.
Se separaron clientes en un extremo del enlace y servidores en otro, se usó una computadora como cliente y una como servidor para realizar las pruebas del servicio de video y de datos, en el caso de telefonía se emplearon teléfonos IP reales y un par de computadoras sólo para poder registrar y comprobar de manera escrita el correcto funcionamientos de dicho canal.
Se reservó un puerto del switch para conectarlo hacia el router, dicho enlace se empleó cómo troncal y se aprovechó para configurar subinterfaces en el puerto ethernet del router.
El otro puerto ethernet del router se conectó hacia la BS en el extremo de los servidores y hacia el SUI en el extremo de los clientes.

La siguiente figura es un diagrama de la topología de la red:

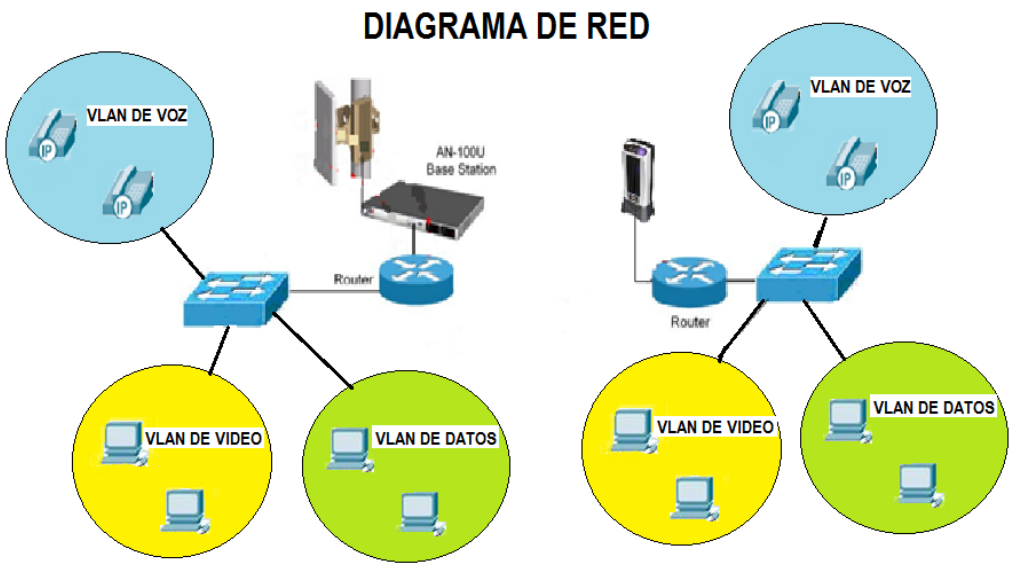


Figura 34 Topología implementada

Y la siguiente tabla describe el direccionamiento IP utilizado:

Dispositivo	Interfaz	IP	Máscara
Teléfono (servidores)	Ethernet	192.168.2.11	255.255.255.0
Servidor de video	Ethernet	192.168.3.11	255.255.255.0
Servidor de datos	Ethernet	192.168.4.11	255.255.255.0
PC (voip)	Ethernet	192.168.2.20	255.255.255.0
Router (servidores)	Subinterfaz de voz	192.168.2.254	255.255.255.0
Router (servidores)	Subinterfaz de video	192.168.3.254	255.255.255.0
Router (servidores)	Subinterfaz de datos	192.168.4.254	255.255.255.0
Router (servidores)	Ethernet 0/1	192.168.182.37	255.255.255.0
BS	Ethernet	192.168.182.3	255.255.255.0
SS	Ethernet	192.168.182.40	255.255.255.0
Router (clientes)	Ethernet 0/1	192.168.182.111	255.255.255.0
Router (clientes)	Subinterfaz de voz	192.168.20.254	255.255.255.0
Router (clientes)	Subinterfaz de video	192.168.30.254	255.255.255.0
Router (clientes)	Subinterfaz de datos	192.168.40.254	255.255.255.0
Teléfono (clientes)	Ethernet	192.168.20.17	255.255.255.0
Cliente de video	Ethernet	192.168.30.17	255.255.255.0
Cliente de datos	Ethernet	192.168.40.17	255.255.255.0
PC (voip)	Ethernet	192.168.20.20	255.255.255.0

Tabla 15 Direccionamiento IP de los dispositivos

5.2 Configuración

La BS cuenta con la opción de deshabilitar flujos de datos sin tener que eliminar los canales, por ello desde un comienzo se crearon todos los flujos a utilizar y estos se activaron o desactivaron en el momento necesario.

Mediante el proceso descrito en el capítulo 3 se configuran los siguientes valores de la interfaz aérea tanto en el suscriptor cómo en la BS:

a) Ancho de banda del canal: 3.5 MHz
b) Frecuencia central de operación: 3478500 Hz
c) Cyclic-Prefix: 1/16

Cómo pasos generales en la BS se desactiva el aprendizaje de MACs para el suscriptor, y en el suscriptor se desactivan los filtrados y el etiquetado de paquetes.

Finalmente se definieron las siguientes clases con sus respectivas características:

Nombre	Tasa reservada	Retardo tolerado	Schedulling
VoIP	128 kbps	30 ms	UGS
Datos	100 kbps	NA	BE
DatosFTP	50-100 kbps	NA	nRTPS
StreamingVideo	3-3.5 Mbps	50 ms	RTPS
CanalUnico	10 Mbps	NA	BE

Tabla 16 Características de las SC programadas

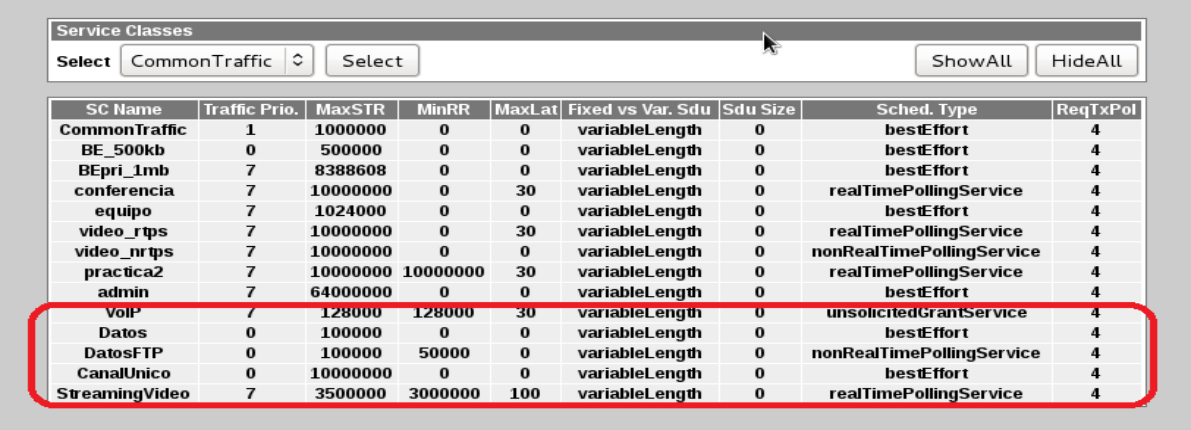
A la voz se le asignó la clase UGS porque esto le garantiza un canal siempre disponible, la desventaja es que esta porción de la tasa de transmisión no está disponible para ningún otro servicio en ningún momento.

Datos es la clase de las peticiones de clientes de video y de datos hacia los servidores, al asignarle la clase BE sí el canal está en desuso puede ser empleado por los otros servicios.

DatosFTP se crea con el tipo nRTPS para que tenga un mínimo de tasa reservado al comenzar la descarga, así el canal aunque se reduzca se mantiene funcionando.

StreamingVideo opera bajo RTPS, esto asegura que cuando haya transmisión de video ningún otro servicio haga bajar su tasa a menos de 3 Mbps (siendo el promedio para este video de 3.5 Mbps) y sí el canal está en desuso puede ser empleado por otro servicio.

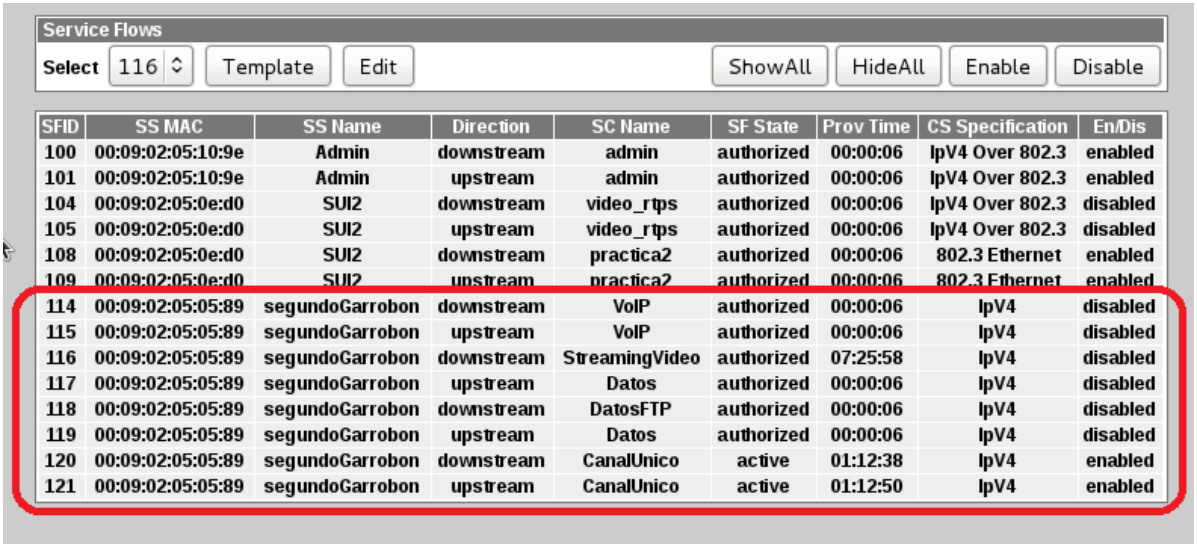
Finalmente CanalUnico se define de 10 Mbps puesto que para el caso en que opera no hay otros flujos activos. La siguiente figura muestra las clases registradas en la BS:



SC Name	Traffic Prio.	MaxSTR	MinRR	MaxLat	Fixed vs Var. Sdu	Sdu Size	Sched. Type	ReqTxPol
CommonTraffic	1	1000000	0	0	variableLength	0	bestEffort	4
BE_500kb	0	500000	0	0	variableLength	0	bestEffort	4
BEpri_1mb	7	8388608	0	0	variableLength	0	bestEffort	4
conferencia	7	10000000	0	30	variableLength	0	realTimePollingService	4
equipo	7	1024000	0	0	variableLength	0	bestEffort	4
video_rtps	7	10000000	0	30	variableLength	0	realTimePollingService	4
video_nrtps	7	10000000	0	0	variableLength	0	nonRealTimePollingService	4
practica2	7	10000000	10000000	30	variableLength	0	realTimePollingService	4
admin	7	64000000	0	0	variableLength	0	bestEffort	4
VoIP	7	128000	128000	30	variableLength	0	unsolicitedGrantService	4
Datos	0	100000	0	0	variableLength	0	bestEffort	4
DatosFTP	0	100000	50000	0	variableLength	0	nonRealTimePollingService	4
CanalUnico	0	10000000	0	0	variableLength	0	bestEffort	4
StreamingVideo	7	3500000	3000000	100	variableLength	0	realTimePollingService	4

Figura 35 SC creadas en la BS

Después de ello se crearon los siguientes SFs:



SFID	SS MAC	SS Name	Direction	SC Name	SF State	Prov Time	CS Specification	En/Dis
100	00:09:02:05:10:9e	Admin	downstream	admin	authorized	00:00:06	IpV4 Over 802.3	enabled
101	00:09:02:05:10:9e	Admin	upstream	admin	authorized	00:00:06	IpV4 Over 802.3	enabled
104	00:09:02:05:0e:d0	SUI2	downstream	video_rtps	authorized	00:00:06	IpV4 Over 802.3	disabled
105	00:09:02:05:0e:d0	SUI2	upstream	video_rtps	authorized	00:00:06	IpV4 Over 802.3	disabled
108	00:09:02:05:0e:d0	SUI2	downstream	practica2	authorized	00:00:06	802.3 Ethernet	enabled
109	00:09:02:05:0e:d0	SUI2	upstream	practica2	authorized	00:00:06	802.3 Ethernet	enabled
114	00:09:02:05:05:89	segundoGarrobon	downstream	VoIP	authorized	00:00:06	IpV4	disabled
115	00:09:02:05:05:89	segundoGarrobon	upstream	VoIP	authorized	00:00:06	IpV4	disabled
116	00:09:02:05:05:89	segundoGarrobon	downstream	StreamingVideo	authorized	07:25:58	IpV4	disabled
117	00:09:02:05:05:89	segundoGarrobon	upstream	Datos	authorized	00:00:06	IpV4	disabled
118	00:09:02:05:05:89	segundoGarrobon	downstream	DatosFTP	authorized	00:00:06	IpV4	disabled
119	00:09:02:05:05:89	segundoGarrobon	upstream	Datos	authorized	00:00:06	IpV4	disabled
120	00:09:02:05:05:89	segundoGarrobon	downstream	CanalUnico	active	01:12:38	IpV4	enabled
121	00:09:02:05:05:89	segundoGarrobon	upstream	CanalUnico	active	01:12:50	IpV4	enabled

Figura 36 SF creados en la BS

Y finalmente los clasificadores:

SFID.ClsID	State	Prio.	Tos Low-High/Mask	DstIp Addr/Mask	SrcIp Addr/Mask	DstPort Start-End	SrcPort Start-End
114.1	inactive	0		192.168.20.0/ 255.255.255.0	192.168.2.0/ 255.255.255.0		
115.1	inactive	0		192.168.2.0/ 255.255.255.0	192.168.20.0/ 255.255.255.0		
116.1	inactive	0		192.168.30.17/ 255.255.255.255	192.168.3.11/ 255.255.255.255		
117.1	inactive	0		192.168.3.11/ 255.255.255.255	192.168.30.17/ 255.255.255.255		
118.1	inactive	0		192.168.40.17/ 255.255.255.255	192.168.4.11/ 255.255.255.255		
119.1	inactive	0		192.168.4.11/ 255.255.255.255	192.168.40.17/ 255.255.255.255		
120.1	active	0					
121.1	active	0					

Figura 36 Clasificadores creados en la BS

5.2.1 Sin QoS

Las configuraciones de equipo CISCO que se mostraran a continuación, son las que se emplearon para todas las pruebas.

5.2.1.1 Configuración del Router conectado a la BS

Se configuro la interfaz Fa0/0 con tres subinterfaces, como se muestra a continuación:

A la interfaz fa0/0 se le asocio a una lista de acceso.

```
interface FastEthernet0/0
no ip address
ip access-group 101 in
duplex auto
speed auto
!
interface FastEthernet0/0.20
encapsulation dot1Q 20
ip address 192.168.2.254 255.255.255.0
!
interface FastEthernet0/0.30
encapsulation dot1Q 30
ip address 192.168.3.254 255.255.255.0
!
interface FastEthernet0/0.40
encapsulation dot1Q 40
ip address 192.168.4.254 255.255.255.0
```

La interfaz fa0/1 va directamente conectada a la BS, por lo cual se le asignó una IP que perteneciera al mismo segmento.

```
!
interface FastEthernet0/1
description Enlace a BS
ip address 192.168.182.37 255.255.255.0
duplex auto
speed auto
```

También se configuraron rutas estáticas, con las cuales se aseguró comunicación con las redes del otro extremo de la red, las redes que van al subscriptor.

```
ip route 192.168.20.0 255.255.255.0 192.168.182.111
ip route 192.168.30.0 255.255.255.0 192.168.182.111
ip route 192.168.40.0 255.255.255.0 192.168.182.111
```

Finalmente se configuraron listas de acceso, para poder asegurar que solo existiera comunicación entre las redes de la misma VLAN.

```
access-list 101 permit ip 192.168.2.0 0.0.0.255 192.168.20.0 0.0.0.255
access-list 101 permit ip 192.168.3.0 0.0.0.255 192.168.30.0 0.0.0.255
access-list 101 permit ip 192.168.4.0 0.0.0.255 192.168.40.0 0.0.0.255
access-list 101 deny   ip any any
```

5.2.1.2 Configuración del Router conectado al Subscriptor

Se configure la interfaz Fa0/0 con tres subinterfaces,como se muestra a continuación:

A la interfaz fa0/0 se le asocio a una lista de acceso.

```
interface FastEthernet0/0
no ip address
ip access-group 100 in
duplex auto
speed auto
!
interface FastEthernet0/0.20
encapsulation dot1Q 20
ip address 192.168.20.254 255.255.255.0
!
interface FastEthernet0/0.30
encapsulation dot1Q 30
ip address 192.168.30.254 255.255.255.0
!
interface FastEthernet0/0.40
encapsulation dot1Q 40
ip address 192.168.40.254 255.255.255.0
```

La interfaz fa0/1 va directamente conectada a la BS, por lo cual se le asigno una IP que perteneciera al mismo segmento.

```
!
interface FastEthernet0/1
description Enlace a subscriptor
ip address 192.168.182.111 255.255.255.0
duplex auto
speed auto
```

También se configuraron rutas estáticas, con las cuales se aseguro comunicación con las redes del otro extremo de la red, las redes que van al subscriptor.

```
ip route 192.168.2.0 255.255.255.0 192.168.182.37
ip route 192.168.3.0 255.255.255.0 192.168.182.37
ip route 192.168.4.0 255.255.255.0 192.168.182.37
```

Finalmente se configuraron listas de acceso, para poder asegurar que solo existiera comunicación entre las redes de la misma VLAN.

```
access-list 100 permit ip 192.168.20.0 0.0.0.255 192.168.2.0 0.0.0.255
access-list 100 permit ip 192.168.30.0 0.0.0.255 192.168.3.0 0.0.0.255
access-list 100 permit ip 192.168.40.0 0.0.0.255 192.168.4.0 0.0.0.255
access-list 101 deny   ip any any
```

5.2.1.3 Configuración del Switch conectado a la BS

Las interfaces de la fa0/1 a la fa0/8 se les asigno la VLAN 20 (VLAN de VOZ), se les configuro en modo de acceso.

```
!
interface FastEthernet0/1
description VLAN_VOZ
switchport access vlan 20
switchport mode access
!
!
interface FastEthernet0/8
description VLAN_VOZ
switchport access vlan 20
switchport mode access
```

Las interfaces de la fa0/9 a la fa0/16 se les asigno la VLAN 30 (VLAN de VIDEO), se les configuro en modo de acceso.

```
interface FastEthernet0/9
description VLAN_VIDEO
switchport access vlan 30
switchport mode access
!
!
```

```
interface FastEthernet0/16
description VLAN_VIDEO
switchport access vlan 30
switchport mode access
```

Las interfaces de la fa0/17 a la fa0/23 se les asigno la VLAN 40 (VLAN de DATOS), se les configuro en modo de acceso.

```
interface FastEthernet0/17
description VLAN_DATOS
switchport access vlan 40
switchport mode access
!
!
interface FastEthernet0/23
description VLAN_DATOS
switchport access vlan 40
switchport mode access
```

La interfaz fa0/24 se configuro como troncal, puesto que esta se conecta como troncal al Router BS.

```
interface FastEthernet0/24
description Trunk a R_BS
switchport mode trunk
!
```

5.2.1.4 Configuración del Switch conectado al Subscriptor

La configuración fue exactamente la misma que la mostrada anteriormente.

- Las interfaces de la fa0/1 a la fa0/8 se les asigno la VLAN 20 (VLAN de VOZ), se les configuro en modo de acceso.

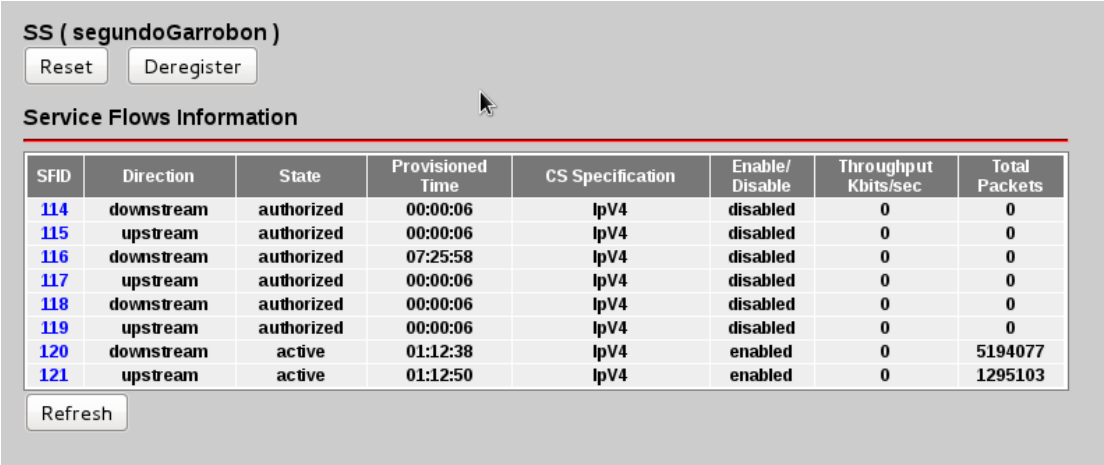
- Las interfaces de la fa0/9 a la fa0/16 se les asigno la VLAN 30 (VLAN de VIDEO), se les configuro en modo de acceso.

- Las interfaces de la fa0/17 a la fa0/23 se les asigno la VLAN 40 (VLAN de DATOS), se les configuro en modo de acceso.

- La interfaz fa0/24 se configuro como troncal, puesto que esta se conecta como troncal al Router del Subscriptor.

5.2.1.5 Configuración de flujos en la BS

Para este caso se ingresa a la pestaña de SFs y se desactivan todos los flujos excepto los correspondientes a la clase canal único, para comprobar que sólo dichos canales funcionen se capturó la pantalla correspondiente al número de paquetes enviados a través de cada canal:


SS (segundoGarrobon)

Reset Deregister

Service Flows Information

SFID	Direction	State	Provisioned Time	CS Specification	Enable/ Disable	Throughput Kbits/sec	Total Packets
114	downstream	authorized	00:00:06	IpV4	disabled	0	0
115	upstream	authorized	00:00:06	IpV4	disabled	0	0
116	downstream	authorized	07:25:58	IpV4	disabled	0	0
117	upstream	authorized	00:00:06	IpV4	disabled	0	0
118	downstream	authorized	00:00:06	IpV4	disabled	0	0
119	upstream	authorized	00:00:06	IpV4	disabled	0	0
120	downstream	active	01:12:38	IpV4	enabled	0	5194077
121	upstream	active	01:12:50	IpV4	enabled	0	1295103

Refresh

Figura 37 Comprobación del uso del canal “Clase Unica”

5.2.2 Con QoS en el equipo CISCO

5.2.2.1 Configuración del Router conectado a la BS

Se crearon tres clases, para cada uno de nuestros servicios (VOZ, VIDEO y DATOS).

A estas clases se les asignaron las listas de acceso previamente configuradas, esto con el objeto de asegurar que las direcciones IP que contienen los distintos paquetes (voz, video y datos) se les asignara la QoS correcta, además, también se les hizo coincidir con los DSCPs (*Differentiated Service Code Point*), asegurando la coincidencia del marcado de los paquetes.

```
class-map VoIP
match access-group 100
match ip dscp ef

class-map VIDEO
match access-group 100
match ip dscp af43

class-map DATOS
```

match access-group 100
match ip dscp af11

Posteriormente se crearon políticas, las cuales se les atribuyeron a las diferentes clases.

A la clase de voz, se le marco con DSCP ef, la cual es la óptima para la voz, tiene una prioridad de valor 5, lo cual hace que sea la primera en enviarse.

También se le asigna una cola de prioridad estricta de 256 kbps y un buffer de 6000 bytes, con lo cual aseguramos suficiente ancho de banda para cuatro llamadas.

policy-map POLITICAS

class VoIP
set ip dscp ef
priority 256 6000

A la clase de video se le etiqueto con un DSCP af43, el cual asegura una prioridad de clase alta, después de la voz, además de que se le reservo un ancho de banda del 60 % de todo el ancho de banda permitido y se activó un mecanismo de descarte inteligente, el cual descarta paquetes con menor valor de DSCP para evitar colisiones, es conocido como WRED(Weighted Random Early Discard).

class VIDEO
set ip dscp af43
bandwidth percent 60
random-detect dscp-based

A la clase de datos se le etiqueto con un DSCP af11, el cual asegura una prioridad de clase baja, puesto que los datos es lo que tiene prioridad más baja en nuestra red, además se le reservo un ancho de banda del 10 % de todo el ancho de banda permitido y se activo un mecanismo de descarte inteligente, igual que en la política de video.

class DATOS
set ip dscp af11
bandwidth percent 10
random-detect dscp-base

Por último se le asignaron las políticas a la salida de la interfaz fa0/1, la cual está conectada a la BS.

interface fa0/1
service-policy output POLITICAS

5.2.2.2 Configuración del Router conectado al Subscriptor

La configuración de QoS debe ser la misma en ambos Routers, por lo cual la configuración aplicada en el Router de la BS, fue la misma en el Router conectado al Subscriptor.

5.2.2.3 Configuración del Switch conectado a la BS

La configuración de QoS a nivel capa 2 solo es necesaria en los puertos que tendrán asignada la VLAN de Voz, en este caso, los puertos Fa0/1 a Fa0/8.

mls qos cos 5, le asigna una prioridad de nivel 5, para la voz.

mls qos trust device cisco-phone, se establece que es un teléfono cisco

mls qos trust cos, se habilita QoS de capa 2

interface FastEthernet0/1
description VLAN_VOZ

5.2.2.4 Configuración del Switch conectado al Subscriptor

switchport access vlan 20
switchport mode access
mls qos cos 5
mls qos trust device cisco-phone
mls qos trust cos

La configuración es exactamente igual al Switch conectado a la BS.

5.2.3 Con QoS de extremo a extremo

En este caso se activan los SF número 114 hasta 119 correspondientes a los canales separados de voz (VoIP), video (VideoStreaming), y datos (datosFTP), a la vez se desactivan los SF 120 y 121 correspondientes al canal único.

Sin embargo el proceso mediante el cual ethernet relaciona direcciones de capa 3 con direcciones de capa 2 (ARP) es usado por los routers por lo que se requiere activar los canales default (Default serviceflows, mencionados también en el capítulo anterior).

CAPITULO VI

Resultados

Este capítulo comienza por realizar pruebas para determinar la máxima tasa de transmisión disponible en el radioenlace para posteriormente saber con que cantidad de información puede saturarse y comenzar a realizar pruebas sobre la degradación de la calidad de los servicios.

Las primeras pruebas se realizan únicamente con el direccionamiento lógico configurado y de forma gradual hasta hacer fallar a los servicios. En seguida se activa la QoS del equipo CISCO con lo que se comparan las mejoras respecto a la situación anterior. Finalmente también se activa la QoS del equipo WiMAX y se realizan un par de pruebas en primer lugar para verificar el correcto funcionamiento de los servicio y en segundo que se cumplan las limitaciones de velocidad de transferencia para los servicios.

6.1 Sin QoS

El tráfico UDP es el que acapara el medio, este se envía sin importar si su información o la de otros servicios es recibida correctamente, el tráfico UDP de mayor volumen es el de video. Por ello para saturar el canal es utilizaron diversas transmisiones de video de manera simultánea, analizando en cada caso las prestaciones del canal respecto al retardo de paquetes, el porcentaje de paquetes recibidos, y el ancho de banda reservado al canal de video. Lo anterior con el fin de mostrar el comportamiento del flujo de datos respecto a las políticas de QoS tanto del equipo de red cableada, como del equipo WiMAX.

Se saturó exclusivamente el canal de bajada debido a que en el extremo de la BS se ubicaron los servidores y en el extremo del suscriptor se ubicaron los clientes.

El enlace implementado atraviesa dos medios de transmisión, el primero cable de red, y el segundo aire. En las interfaces ethernet se tuvo una velocidad de enlace de 100 Mbps en modo full duplex, mientras que en la interfaz aérea fue de 6.6 Mbps en el canal de bajada y de 4.5 Mbps en el canal de subida. La siguiente figura indica dichos valores:

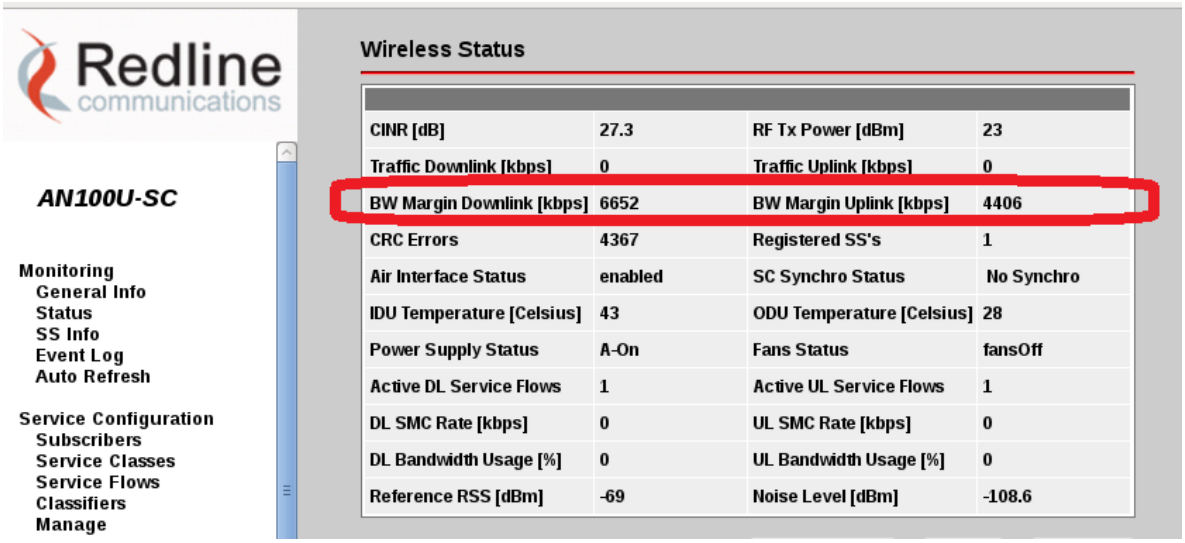


Figura 38 Máxima tasa de transmisión indicada por la BS

Teniendo en cuenta que la velocidad de procesamiento en el equipo de red es mayor a la de sus interfaces, la velocidad de transmisión alcanzada de extremo a extremo está limitada por la velocidad de transmisión de la interfaz aérea. Para comprobar esto se usó un analizador de tráfico.

6.1.1 Velocidad de transmisión máxima del canal de bajada (de extremo a extremo):

El valor de la velocidad de transmisión soportado por la BS fue de 6.6 Mbps, y el valor promedio del video utilizado fu de 2.5 Mbps así que usando sólo las computadoras correspondientes al servicio de video se transmitieron de manera paralela 5 videos, prestando atención a la velocidad de transmisión indicada por el analizador de red en el extremo receptor. Dicho valor es el mostrado en la siguiente figura:

Network Load	Actual	6.1 Mbit/s	581.6 Pkt/s
	Last Minute	6.1 Mbit/s	587.6 Pkt/s
	Last 5 Minutes	5.9 Mbit/s	564.4 Pkt/s
	Peak	6.5 Mbit/s	626.4 Pkt/s
	Average	4.7 Mbit/s	447.3 Pkt/s
Historical Data			[ ]

Global Protocol Distribution

Protocol	Data	Percentage				
IP	969.6 MBytes	100.0%	UDP	968.9 MBytes	99.9%	
			ICMP	740.2 KBytes	0%	

Figura 39 Comprobación de la máxima tasa de transmisión mediante NTOP

6.1.2 Análisis 1 Retardo en el canal de voz sin trafico en los demas segmentos

Para determinar las pérdidas que se presentan de extremo a extremo de nuestra red, se utilizó el comando ping. Para la primera prueba se hizo ping desde el Router del Subscriptor hacia una IP del segmento de la VLAN de VOZ, para poder determinar las pérdidas de paquetes y los problemas de latencia; con el objeto de asegurar que los retardos no superen los 126 ms que son los necesarios para una llamada de voz.

Las tres pruebas que se realizaron, fueron las mismas para todos análisis.

Primera prueba:

Ping 192.168.2.11 repeat 1000

El router Cisco envía 1000 paquetes tan rápido como se puedan generar, esperando respuestas.

```
R_Subscriptor#ping 192.168.2.11 repeat 1000

Type escape sequence to abort.
Sending 1000, 100-byte ICMP Echos to 192.168.2.11, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!
Success rate is 99 percent (999/1000), round-trip min/avg/max = 28/30/32 ms
```

Figura 40 Respuesta ICMP del Router (ping repetido 1000)

La figura muestra que los 999 paquetes obtuvieron respuestas, salvo un paquete, con tiempos mínimos de 28ms y máximos de 32ms.

Segunda prueba:

Ping 192.168.2.11 size 1000

Se crea un paquete ICMP de tamaño 1000

```
R_Subscriptor#ping 192.168.2.11 size 1000

Type escape sequence to abort.
Sending 5, 1000-byte ICMP Echos to 192.168.2.11, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 40/40/40 ms
```

Figura 41 Respuesta ICMP del Router (tamaño paquete ICMP 1000)

Se observa que la respuesta de eco fue recibida correctamente, con un mínimo y máximo de 40ms.

Tercera prueba:

Se realizó un ping desde una computadora hacia otra computadora.

Se generó un ping que se repitió 40 veces.

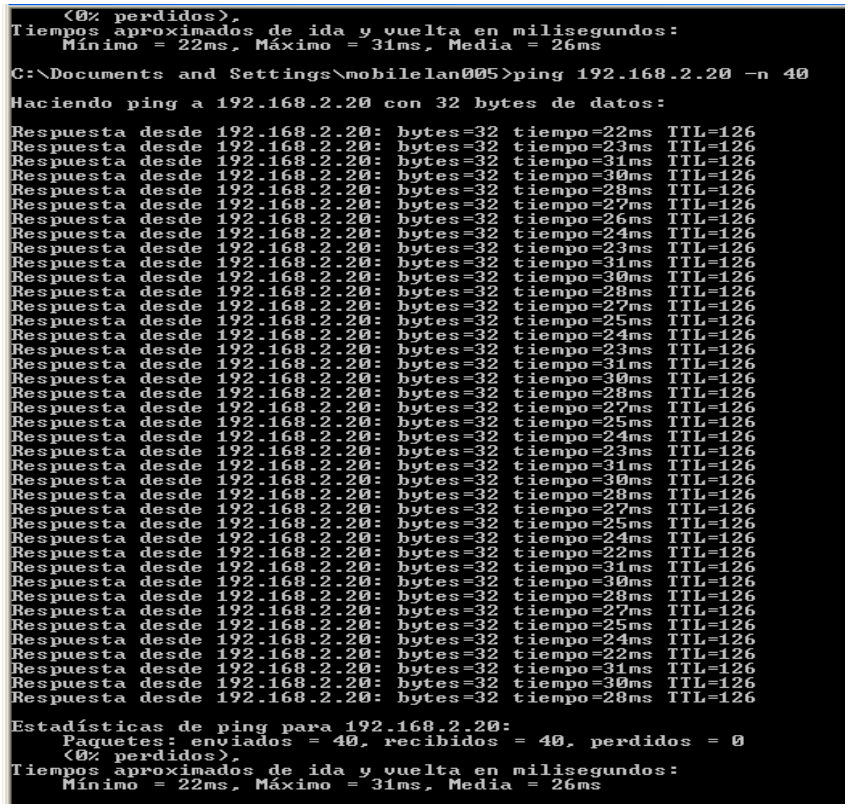


Figura 42 Respuesta ping de PC de voz

Se puede observar que no hubo pérdidas en los pings, se mandaron 40 pings y se recibieron 40 pings, además se tuvo un mínimo de 22ms y un máximo de 31ms en la respuesta de estos.

La siguiente gráfica muestra los retardos producidos de la anterior prueba.

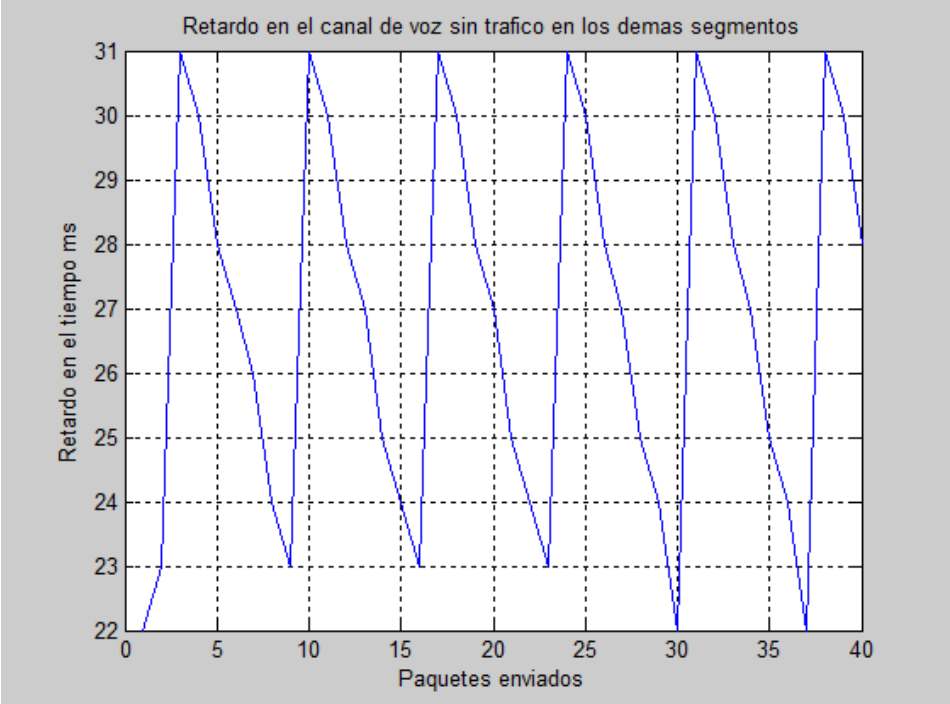


Figura 43 Gráfica de los retardos de los paquetes ping

Se observa que los retardos oscilan entre 22ms y 31 ms

6.1.3 Análisis 2. Retardo en el canal de voz inyectando tráfico en el canal de datos mediante el software IPER

Primera prueba:

Ping 192.168.2.11 repeat 1000

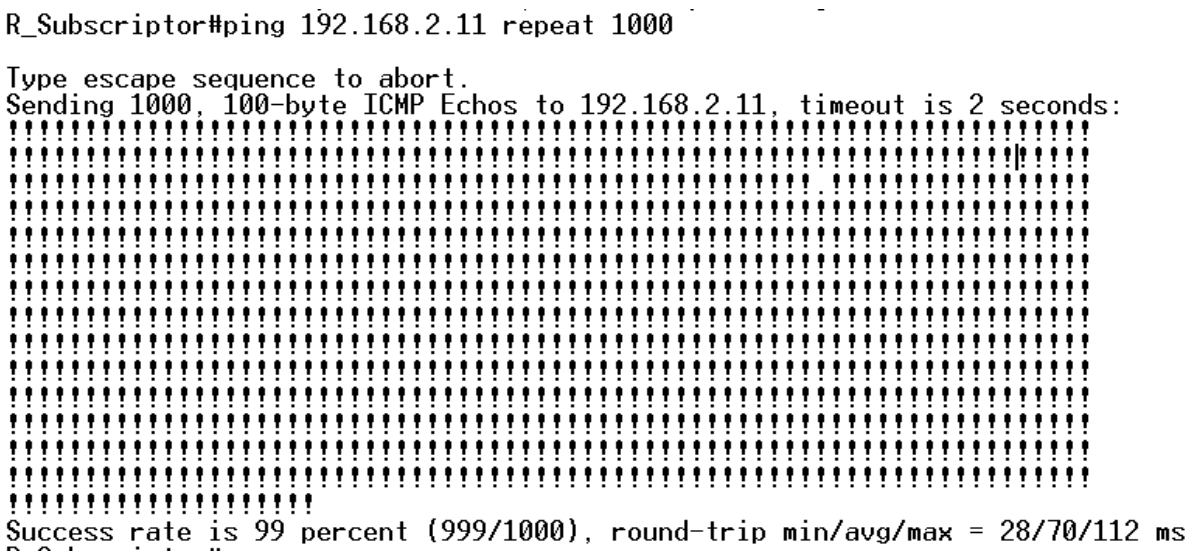


Figura 44 Respuesta ICMP del Router (ping repetido 1000)

La figura muestra que los 999 paquetes obtuvieron respuestas, salvo un paquete, con tiempos mínimos de 28ms y máximos de 112ms.

Para este caso se puede observar que el tiempo de latencia subió hasta 112ms como máximo, teniendo en cuenta que en la primer análisis sin tráfico agregado fue de 32ms.

Segunda prueba:

Ping 192.168.2.11 size 1000

Se crea un paquete ICMP de tamaño 1000

```
R_Subscriptor#ping 192.168.2.11 size 1000
Type escape sequence to abort.
Sending 5, 1000-byte ICMP Echos to 192.168.2.11, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 36/91/120 ms
```

Figura 45 Respuesta ICMP del Router (tamaño paquete ICMP 1000)

En este caso la respuesta de eco fue recibida correctamente, con un mínimo de 36 ms y un máximo de 120ms.

Tercera prueba:

Se realizó un ping desde una computadora hacia otra computadora.

Se generó un ping que se repitió 40 veces.

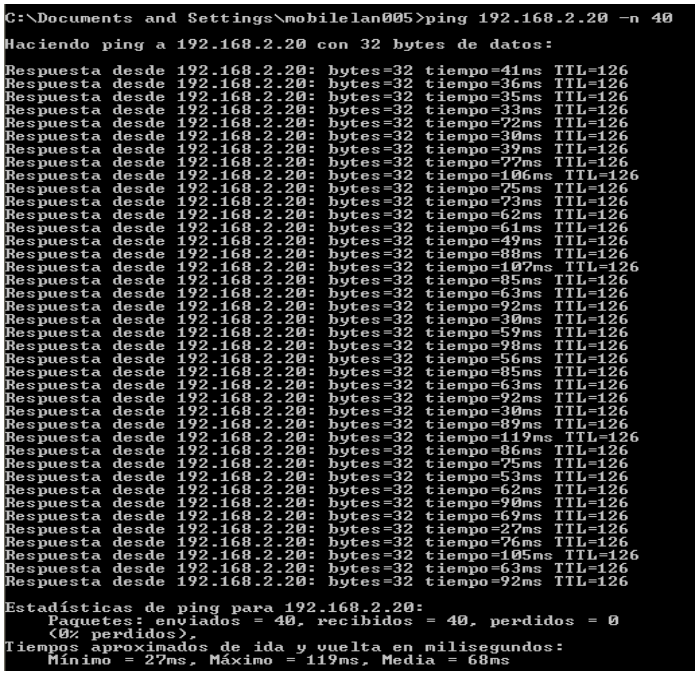


Figura 46 Respuesta ping de PC de voz

Tampoco hubo pérdidas en los pings, se mandaron 40 pings y se recibieron 40 pings, pero la latencia está incrementándose, con mínimo de 27ms y máximo de 119ms en la respuesta de estos.

La siguiente gráfica muestra los retardos producidos de la anterior prueba.

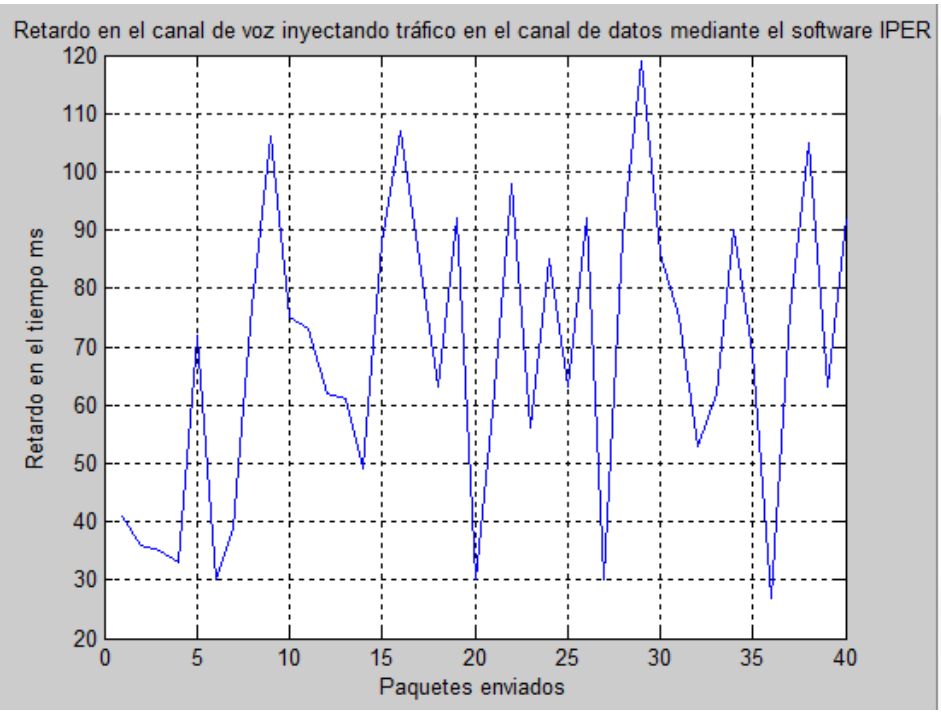


Figura 46 Gráfica de los retardos de los paquetes ping

La grafica ilustra la variación del tiempo de respuesta que se da al inyectar tráfico.

6.1.4 Análisis 3. Retardo en el canal de voz inyectando tráfico en el canal de datos mediante el software IPER e inyectando tráfico en el canal de video, mediante la descarga de un video

Primera prueba:

Ping 192.168.2.11 repeat 1000

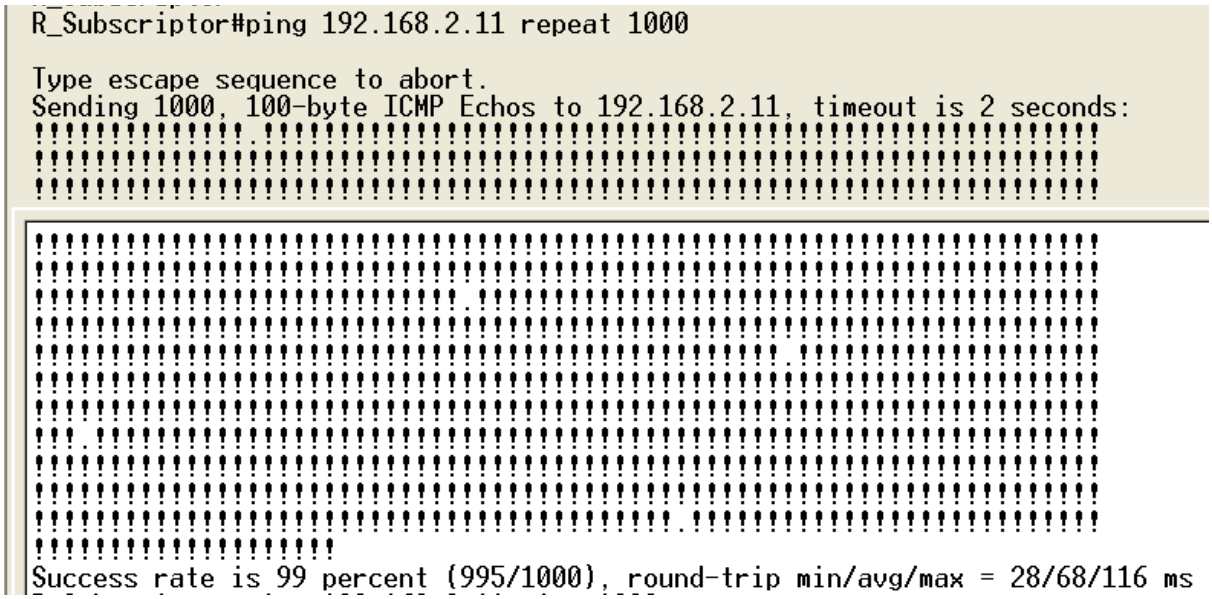


Figura 48 Respuesta ICMP del Router (ping repetido 1000)

En este caso ya hay un incremento en la perdida de paquetes, 5 en este caso, además de que la latencia sigue incrementándose.

Segunda prueba:

Ping 192.168.2.11 size 1000

Se crea un paquete ICMP de tamaño 1000

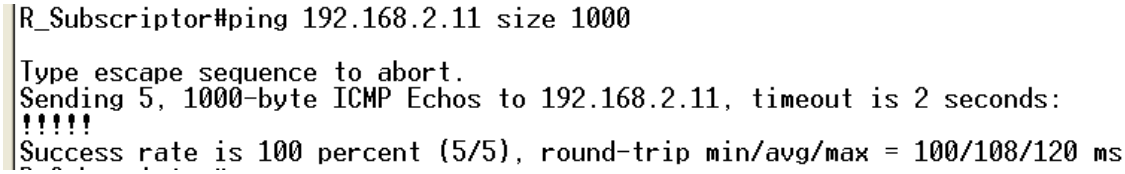


Figura 49 Respuesta ICMP del Router (tamaño paquete ICMP 1000)

Las respuestas de eco se siguen recibiendo, pero los tiempos de respuesta ya aumentaron más, puesto que el mínimo se obtuvo en 100ms y el máximo en 120ms.

Tercera prueba:

Se realizó un ping desde una computadora hacia otra computadora.

Se generó un ping que se repitió 40 veces.

Figura 50 Respuesta ping de PC de voz

Los paquetes ICMP llegaron completos, pero los retardos siguen incrementándose, mínimo de 46 ms y máximo de 116 ms

La siguiente gráfica muestra los retardos producidos de la anterior prueba.

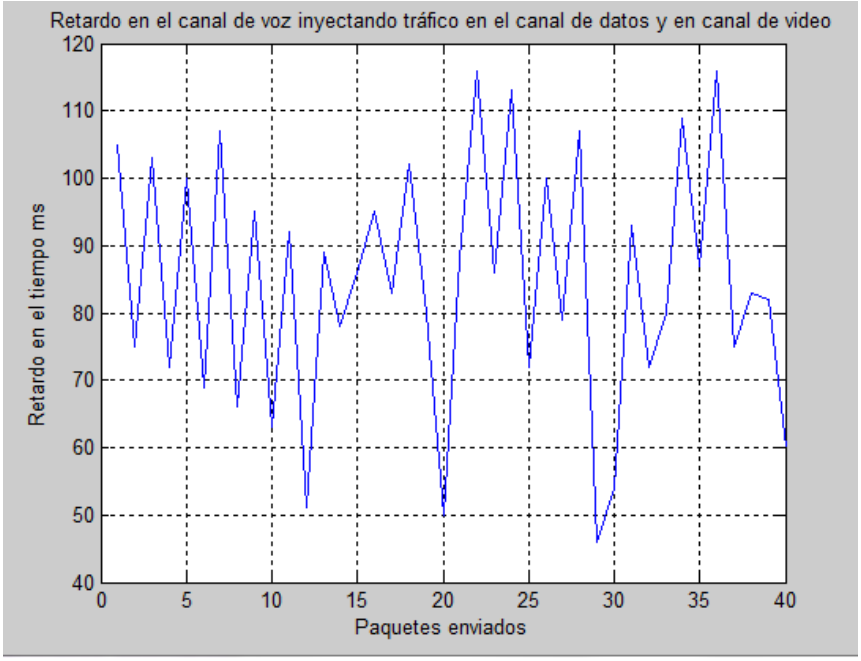


Figura 51 Gráfica de los retardos de los paquetes ping

La grafica muestra que los retardos en el tiempo cambian más en comparación con las anteriores.

Por otra parte el video se reprodujo en su mayoría sin pausas ni distorsiones, la siguiente imagen es una captura hecha en el cliente:

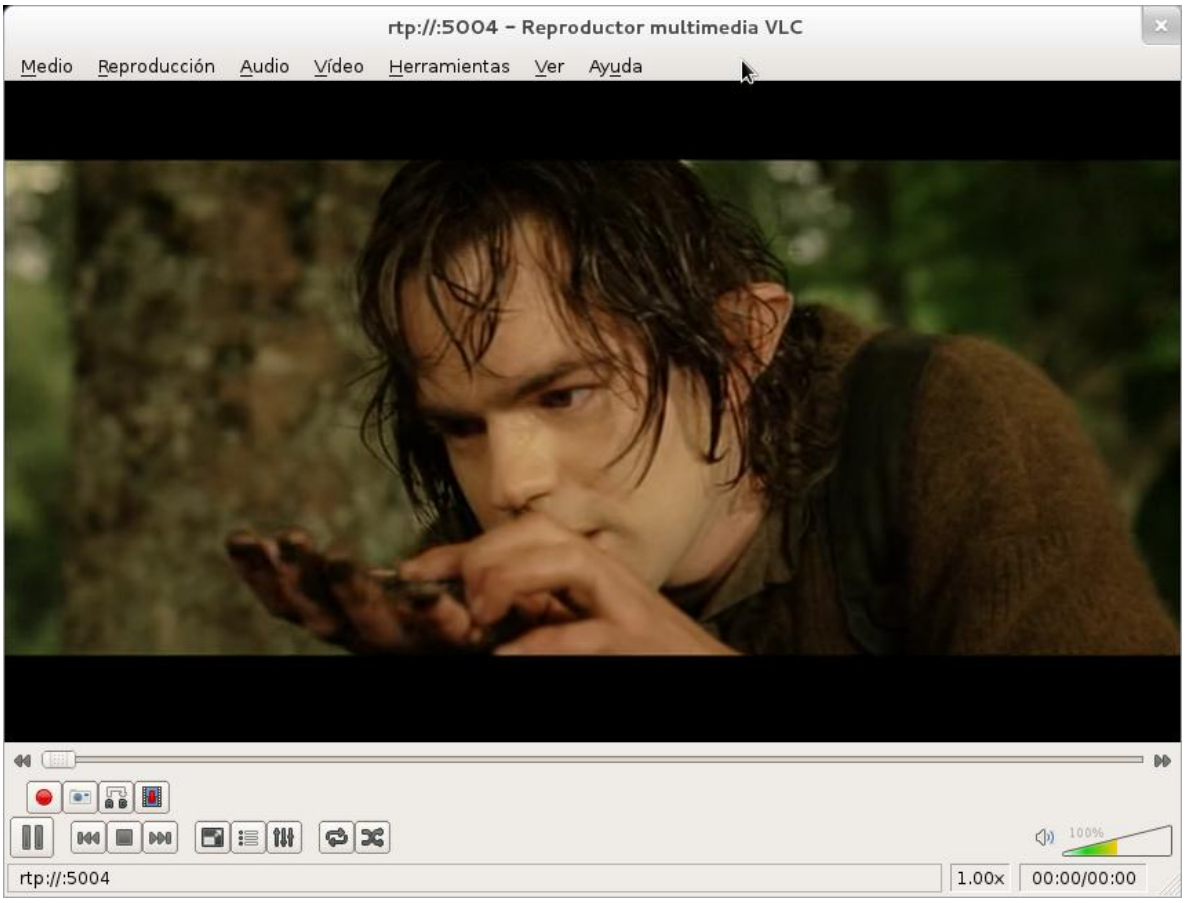


Figura 52 Imagen de un video transmitiéndose

Mediante nTop registramos el siguiente valor de tasa de transmisión en el cliente de video:

Network Load	Actual	2.6 Mbit/s	253.0 Pkt/s
	Last Minute	0.0 bit/s	0.0 Pkt/s
	Last 5 Minutes	0.0 bit/s	0.0 Pkt/s
	Peak	2.6 Mbit/s	253.0 Pkt/s
	Average	2.5 Mbit/s	236.7 Pkt/s
Historical Data			[ ]

Figura 53 Tasa de transmisión para un video

6.1.5 Análisis 4. Retardo en el canal de voz inyectando tráfico en el canal de datos mediante el software IPER he inyectando tráfico en el canal de video, mediante la descarga de 2 videos

Primera prueba:

Ping 192.168.2.11 repeat 1000

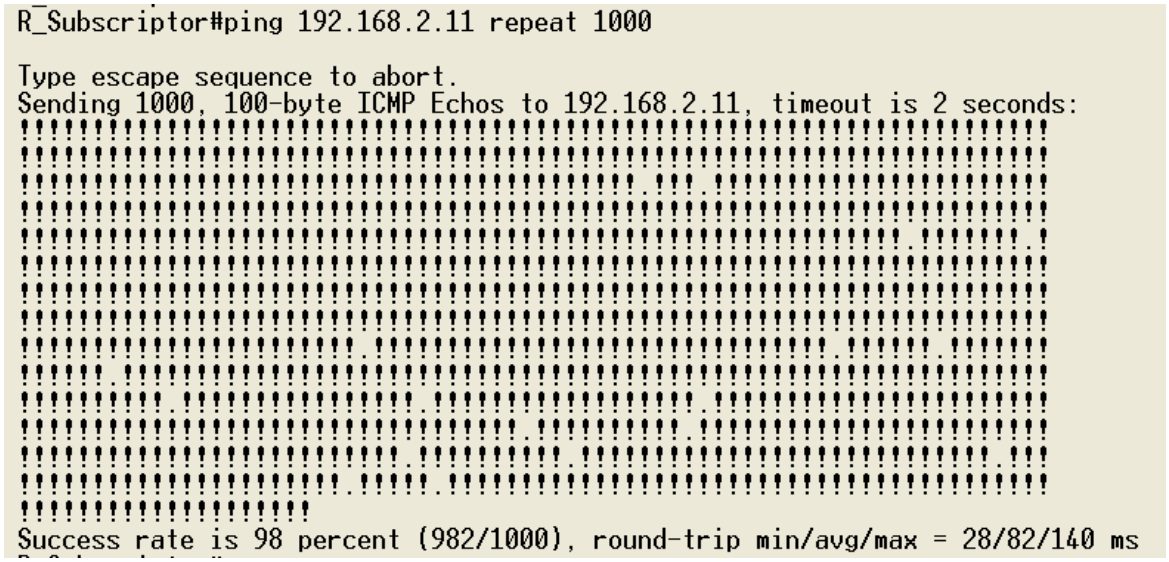


Figura 54 Respuesta ICMP del Router (ping repetido 1000)

Se observa con mas claridad los paquetes perdidos (18 paquetes), ademas de que la latencia se incremento a 140 ms como maxima.

Segunda prueba:

Ping 192.168.2.11 size 1000

Se crea un paquete ICMP de tamaño 1000

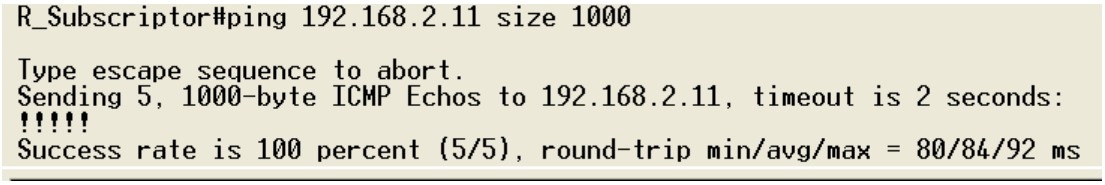


Figura 55 Respuesta ICMP del Router (tamaño paquete ICMP 1000)

Los paquetes ICMP llegaron completos, pero el tiempo mínimo de latencia se incremento a 80 ms, y el tiempo máximo bajo a 92 ms, este resultado no se esperaba.

Tercera prueba:

Se realizó un ping desde una computadora hacia otra computadora.

Se generó un ping que se repitió 60 veces.

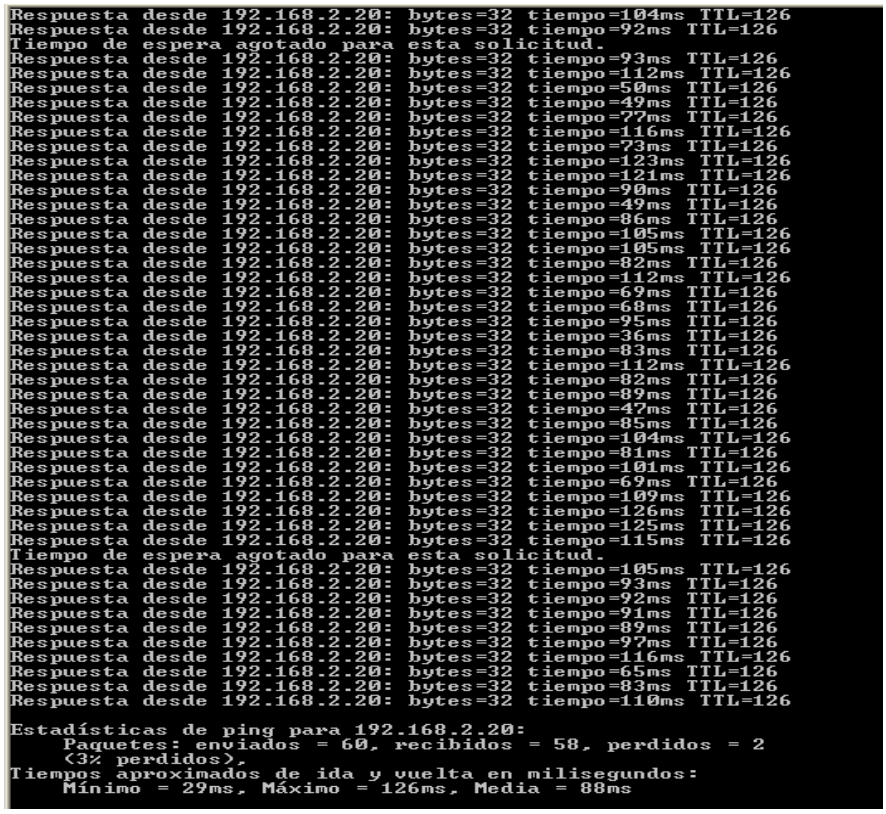


Figura 56 Respuesta ping de PC de voz

En esta prueba ya empieza a ver pérdidas de paquetes (2 paquetes).

La siguiente gráfica muestra los retardos producidos de la anterior prueba.

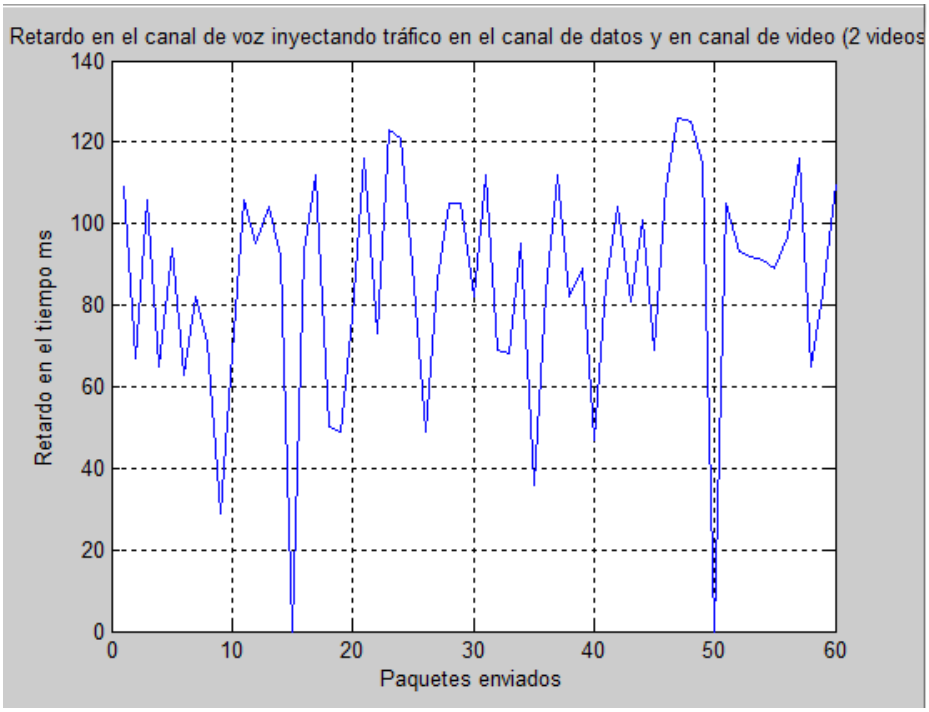


Figura 57 Gráfica de los retardos de los paquetes ping

La grafica muestra dos caídas, que significan que los pings no tuvieron respuesta.

El video comenzó a sufrir distorsiones; Sin embargo aún no se producían pausas. La siguiente imagen es una captura de video en el cliente:

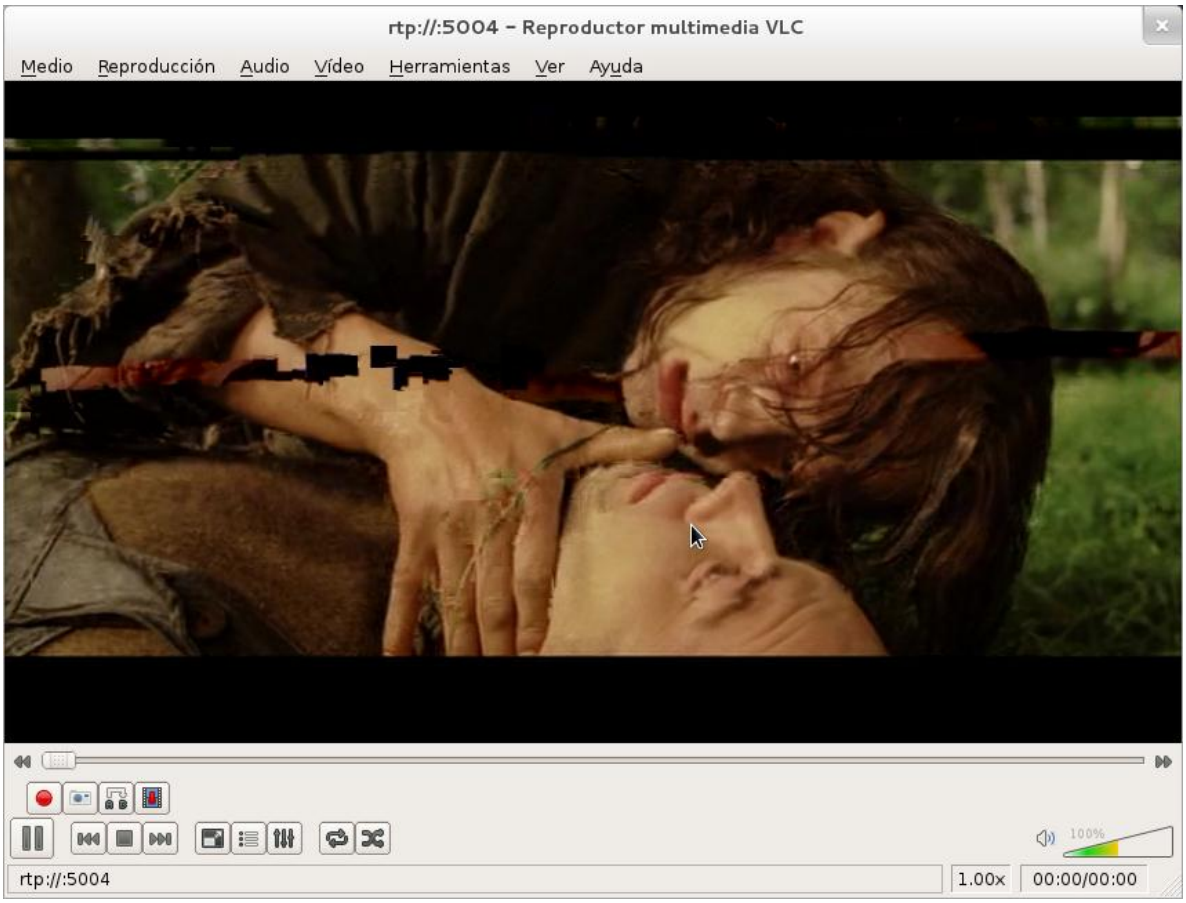


Figura 58 Imagen de dos videos transmitiéndose

De nueva cuenta se analizó nTop y se observó que es este servicio el que acapara el canal:

Network Load	Actual	5.9 Mbit/s	563.6 Pkt/s
	Last Minute	5.5 Mbit/s	531.8 Pkt/s
	Last 5 Minutes	3.8 Mbit/s	368.4 Pkt/s
	Peak	6.2 Mbit/s	593.0 Pkt/s
	Average	3.8 Mbit/s	367.9 Pkt/s
Historical Data			[ ]

Figura 59 Tasa de transmisión para dos videos

6.1.6 Análisis 5. Retardo en el canal de voz inyectando tráfico en el canal de datos mediante el software IPERF e inyectando tráfico en el canal de video, mediante la descarga de 3 videos

Primera prueba:

Ping 192.168.2.11 repeat 1000

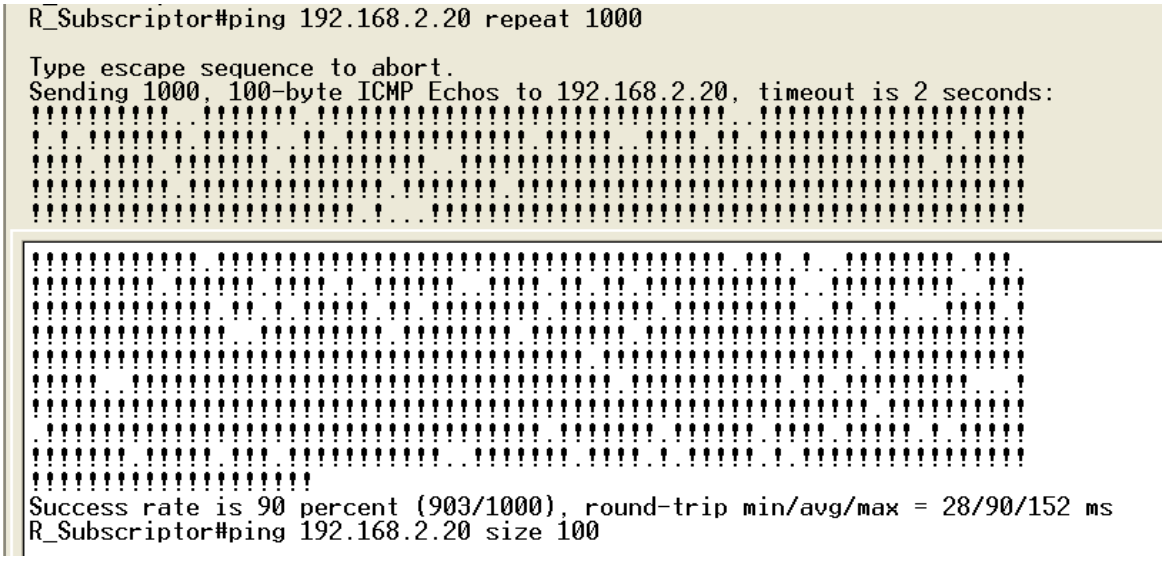


Figura 60 Respuesta ICMP del Router (ping repetido 1000)

Con tres videos se puede observar quehay mas perdidas de paquetes (97 paquetes), con incrementos de retardos de 152 ms.

Segunda prueba:

Ping 192.168.2.11 size 1000

Se crea un paquete ICMP de tamaño 1000

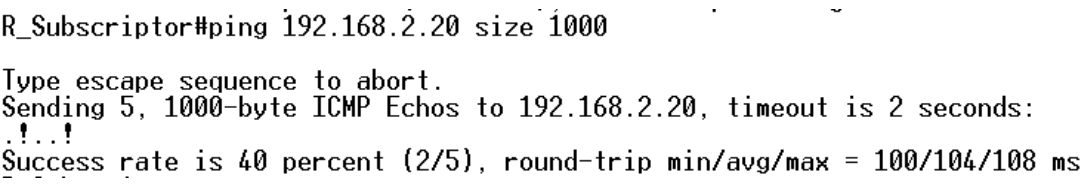


Figura 61 Respuesta ICMP del Router (tamaño paquete ICMP 1000)

De 5 paquetes ICMP llegaron solo 3, y los tiempos de latencia son elevados, el mínimo y el máximo son muy parecidos, 100ms y 108 ms respectivamente.

Tercera prueba:

Se realizó un ping desde una computadora hacia otra computadora.

Se genero un ping que se repitió 40 veces.

Figura 62 Respuesta ping de PC de voz

Se muestran mas perdidas de paquetes ping (4 paquetes), por otro lado, la latencia sigue respetando el mismo sentido que en la anterior prueba.

La siguiente gráfica muestra los retardos producidos de la anterior prueba.

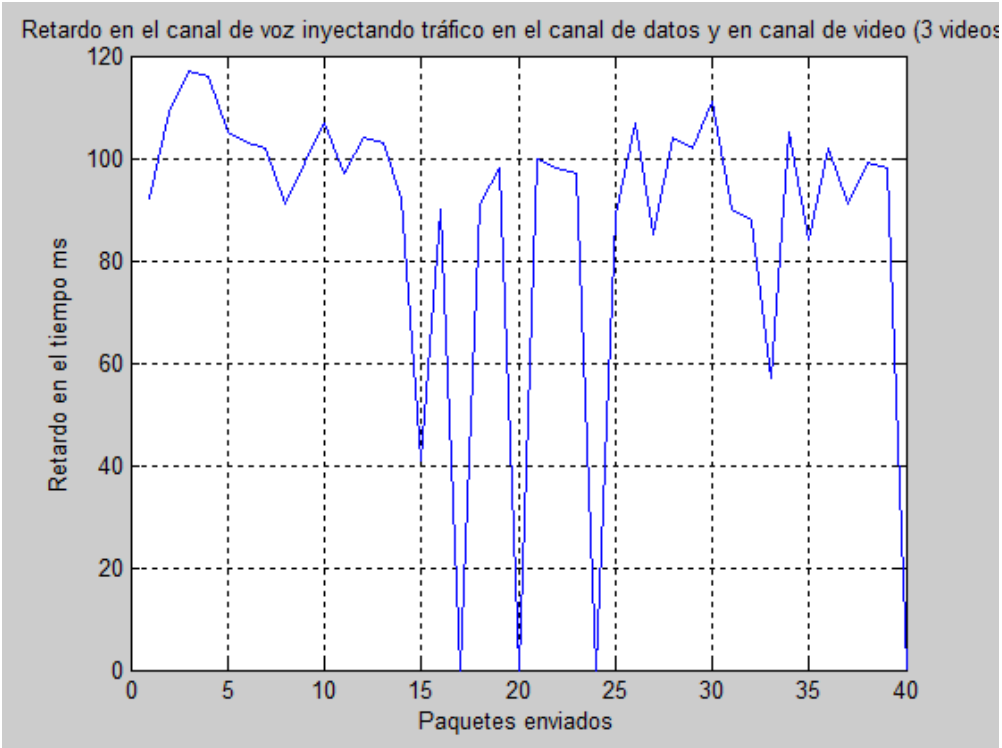


Figura 63 Gráfica de los retardos de los paquetes ping

Se muestran 4 caidas, las cuales significan que 4 paquetes ICMP no tuvieron respuesta de eco.

El video comenzó a sufrir pausas además de distorisón, la siguiente imagen es una catura del video en el cliente:

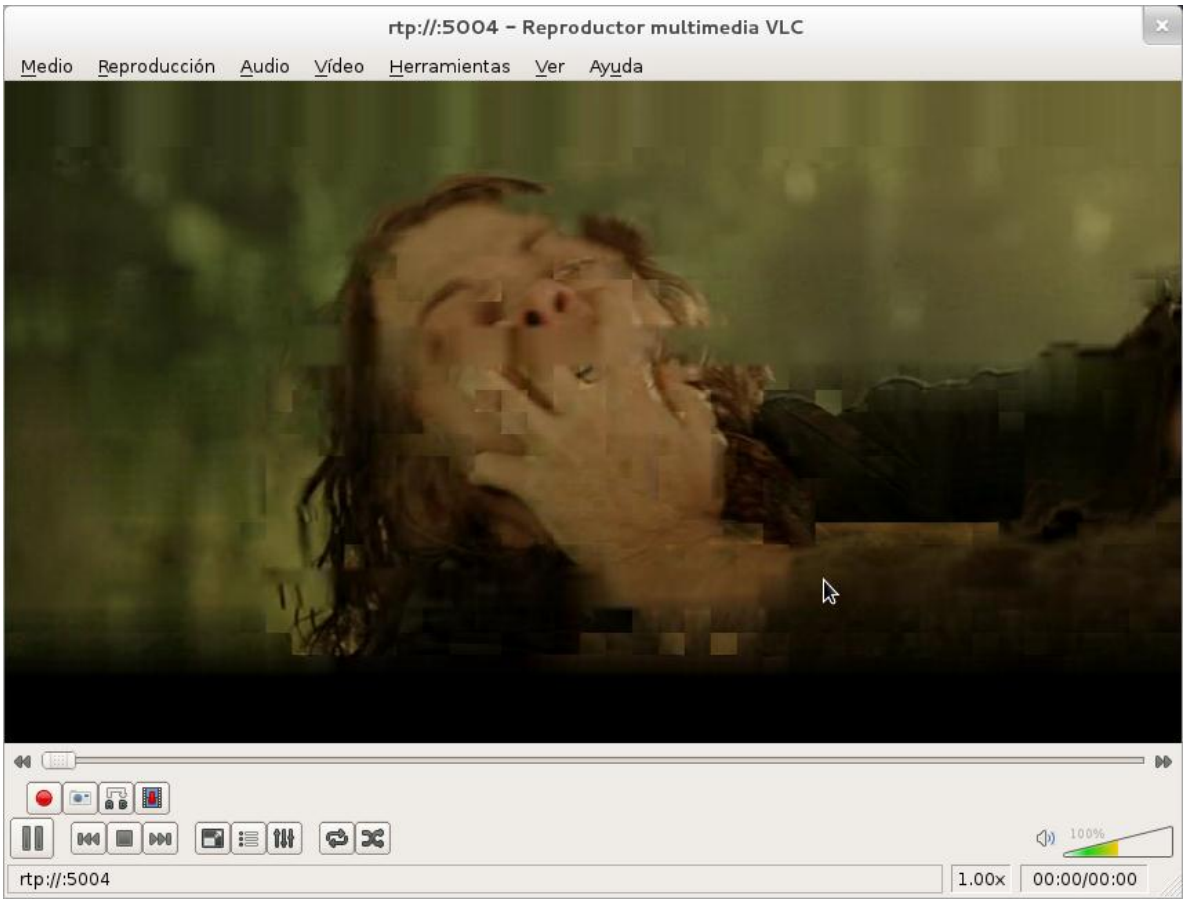


Figura 64 Imagen de tres videos transmitiéndose

Con nTop se observó que a pesar de las distorsiones y pausas aún no se llegaba al límite del enlace:

Network Load	Actual	6.0 Mbit/s	572.0 Pkt/s
	Last Minute	6.3 Mbit/s	602.5 Pkt/s
	Last 5 Minutes	0.0 bit/s	0.0 Pkt/s
	Peak	6.4 Mbit/s	618.0 Pkt/s
	Average	6.1 Mbit/s	589.7 Pkt/s
Historical Data			

Figura 65 Tasa de transmisión para tres videos

6.1.7 Análisis 6. Retardo en el canal de voz inyectando tráfico en el canal de datos mediante el software IPER e inyectando tráfico en el canal de video, mediante la descarga de 4 videos

Primera prueba:

Ping 192.168.2.11 repeat 1000

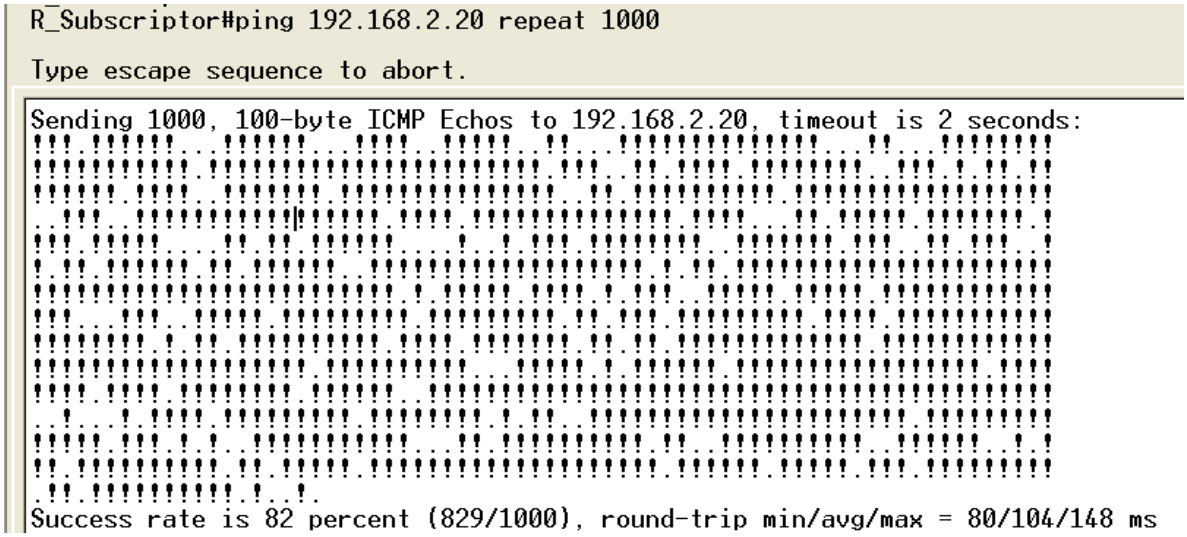


Figura 66 Respuesta ICMP del Router (ping repetido 1000)

Las perdidas de paquetes ya son muchas (171 paquetes), los retardos son grandes tambien.

Segunda prueba:

Ping 192.168.2.11 size 1000

Se crea un paquete ICMP de tamaño 1000

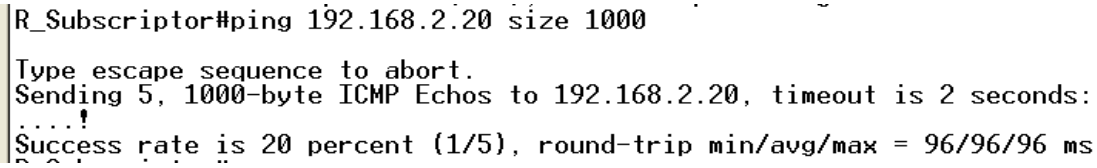


Figura 67 Respuesta ICMP del Router (tamaño paquete ICMP 1000)

En este caso solo un paquete llego, y los retardos minimo y maximo son iguales.

Tercera prueba:

Se realizó un ping desde una computadora hacia otra computadora.

Se generó un ping que se repitió 60 veces.

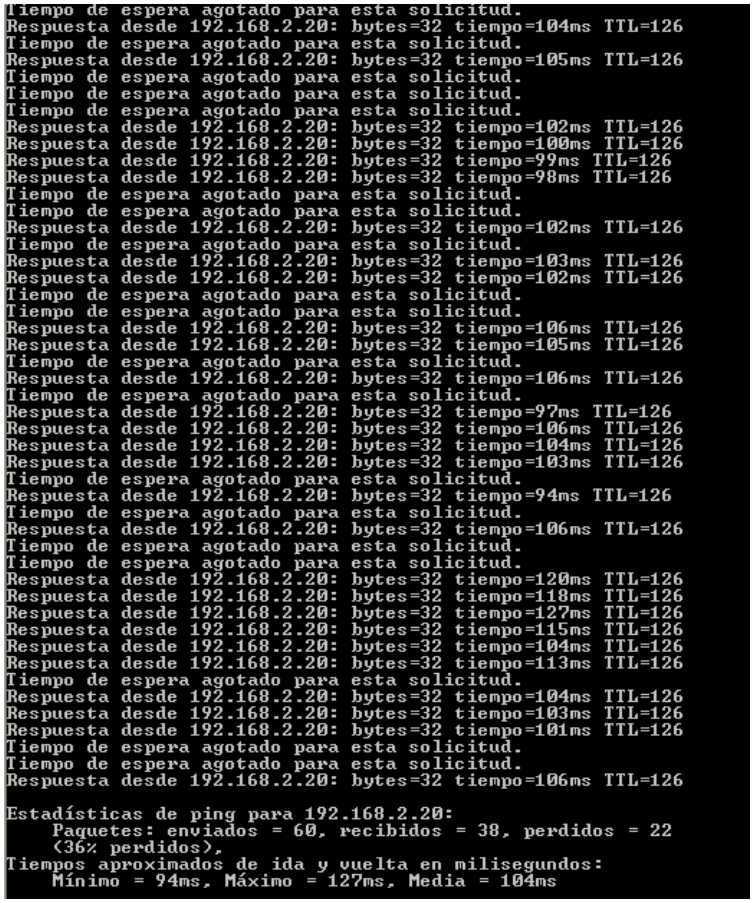


Figura 68 Respuesta ping de PC de voz

Se perdieron muchos paquetes ping (22 paquetes) de 60 enviados, ademas de que los retardos incrementaron.

La siguiente gráfica muestra los retardos producidos de la anterior prueba.

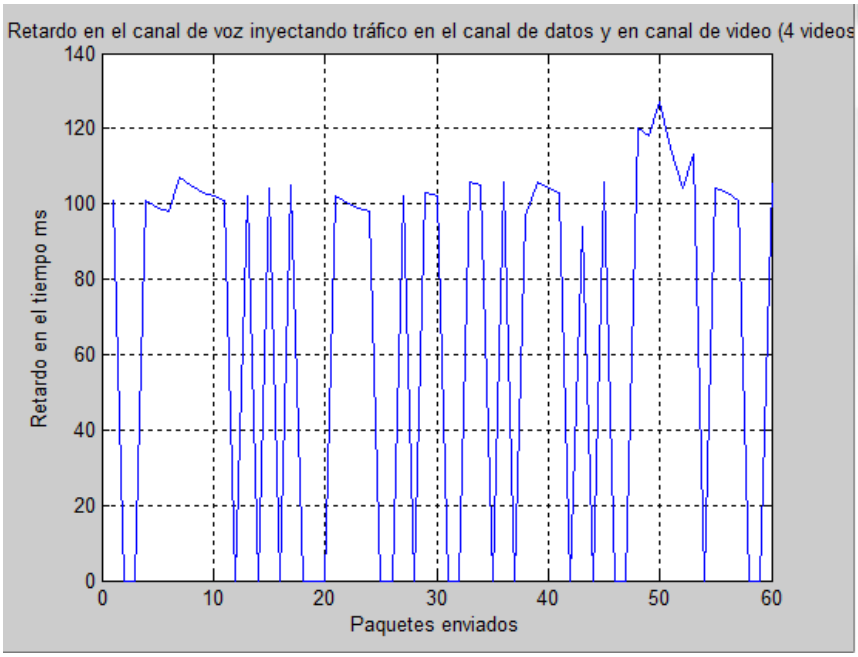


Figura 69 Gráfica de los retardos de los paquetes ping

Se observan muchas caidas de mensajes ICMP, ya que estos no tuvieron respuesta de eco.

En este caso el video tanto en audio como en video dejó de ser legible completamente, la siguiente imagen es un captura del video en el cliente:

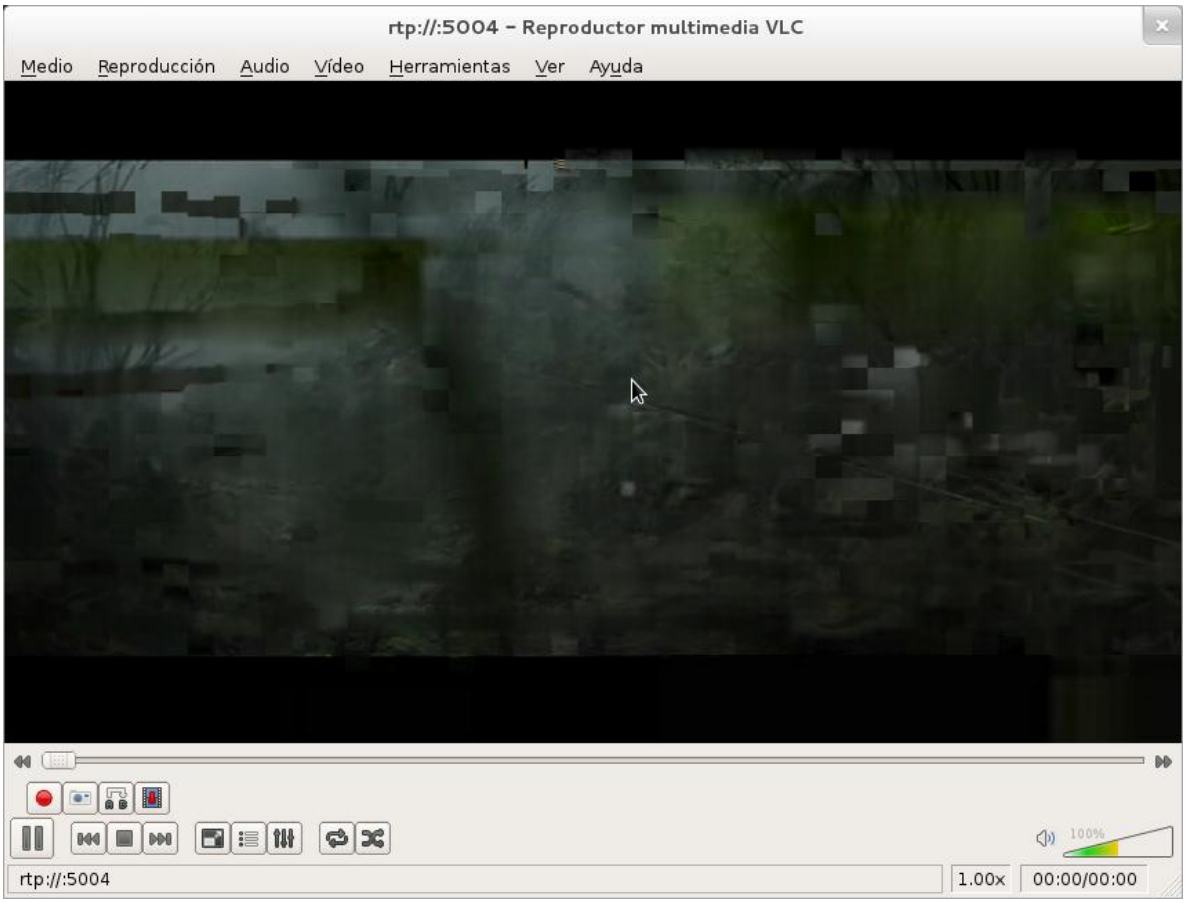


Figura 70 Imagen de cuatro videos transmitiéndose

nTop muestra que se está muy próximo a la saturación del enlace, si no se alcanza es debido a que la tasa de transmisión de los videos es variable y la mayoría de ellos estaba en valores mínimos:

Network Load	Actual	6.4 Mbit/s	615.9 Pkt/s
	Last Minute	6.3 Mbit/s	602.5 Pkt/s
	Last 5 Minutes	0.0 bit/s	0.0 Pkt/s
	Peak	6.4 Mbit/s	618.0 Pkt/s
	Average	6.2 Mbit/s	595.0 Pkt/s
Historical Data			[ ]

Figura 71 Tasa de transmisión para cuatro videos

Cabe destacar que al inyectar tráfico mediante iPERF dicho programa presentó fallas, en repetidas ocasiones no fue capaz de completar la conexión, se capturó la siguiente imagen de dicho evento:

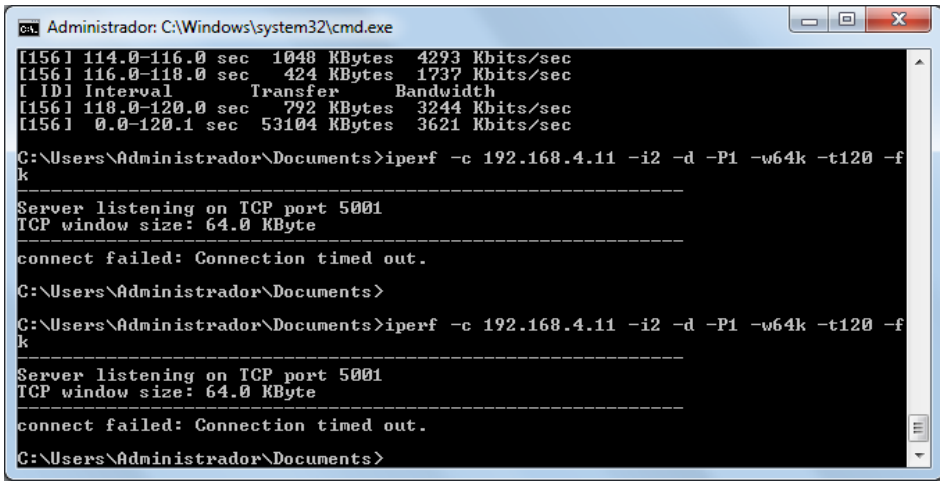


Figura 72 Falló del programa iPERF

6.1.8 Análisis 7. Retardo en el canal de voz inyectando tráfico en el canal de video, mediante la descarga de 5 videos

Una vez comprobado que el tráfico TCP tuvo deificultades de operación se prosiguió por transmitir un video más con el fin de comparar la tasa máxima que podía alcanzar dicho servicio cuando se ocupaban los otros (a pesar de que fallaran).

El video como se esperaba fue completamante distorsionado:

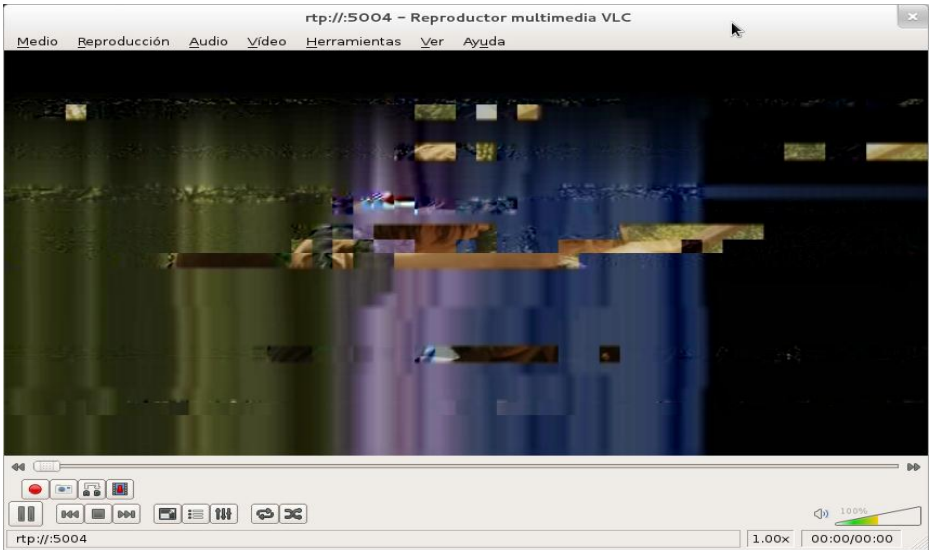


Figura 73 Imagen de cinco videos transmitiéndose

En este caso nTop registró un máximo de 6.4 Mbps en comparación con los 6.5 Mbps alcanzados en un comienzo esto debido al tráfico que se intentó enviar por TCP.

Network Load	Actual	6.3 Mbit/s	605.0 Pkt/s
	Last Minute	6.2 Mbit/s	593.3 Pkt/s
	Last 5 Minutes	0.0 bit/s	0.0 Pkt/s
	Peak	6.4 Mbit/s	618.0 Pkt/s
	Average	6.2 Mbit/s	594.8 Pkt/s
Historical Data			[ ]

Figura 74 Tasa de transmisión para cinco videos

Como observación en todo momento probamos los teléfonos IP a la vez que se probaban los pings, nunca se perdió la comunicación de voz a pesar de la pérdida de paquetes. Lo anterior pudo deberse a la cercanía entre los equipos WiMAX que evitó que se produjera un retraso mayor a 150 ms, por otra parte se comprobó que este servicio es robusto contra la perdidad moderada de paquetes.

6.2 Con QoS en el equipo CISCO

Se realizó la simulación únicamente transmitiendo al mismo tiempo 4 videos debido a que en el caso anterior fue con esta cantidad que falló el servicio de tcp (iPerf), además de obtener una velocidad de transmisión constante en el analizador de red que es un indicador de haber saturado el canal.

La imagen de video siguió estando degradada debido a la saturación del enlace; Sin embargo iPerf volvió a funcionar y se presentaron mejoras respecto al retardo y la pérdida de paquetes en el canal de voz. Los resultados se muestran a continuación:

6.2.1 Análisis 1. Retardo en el canal de voz inyectando tráfico en el canal de datos mediante el software IPERF e inyectando tráfico en el canal de video, mediante la descarga de 4 videos

Primera prueba:

Ping 192.168.2.11 repeat 1000

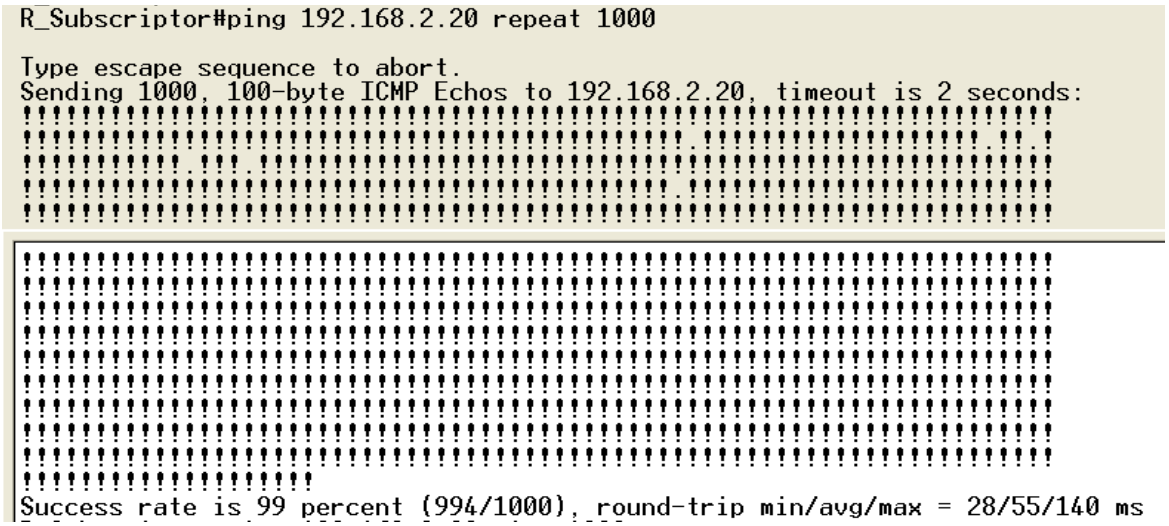


Figura 75 Respuesta ICMP del Router (ping repetido 1000)

Al comparar esta salida con la mostrada en el análisis 6, se puede observar una gran mejora, solo se pierden 6 paquetes, puesto que la QoS empleada está etiquetando los paquetes, haciendo que se reserve un ancho de banda y una prioridad a cada servicio.

Segunda prueba

Ping 192.168.2.11 size 1000

Se crea un paquete ICMP de tamaño 1000

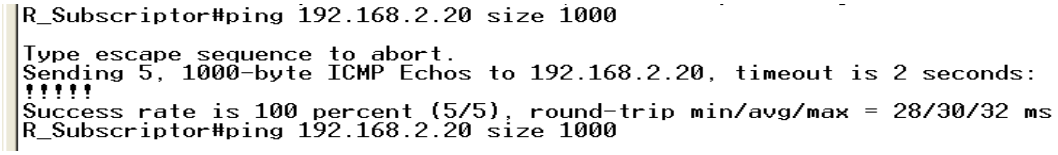


Figura 76 Respuesta ICMP del Router (tamaño paquete ICMP 1000)

También esta prueba muestra que ningún paquete ICMP fue perdido, además de que los retrasos de latencia son muy bajos.

Tercera prueba:

Se realizó un ping desde una computadora hacia otra computadora.

Se generó un ping que se repitió 40 veces.

```
C:\Documents and Settings\mobilelan005>ping 192.168.2.20 -n 40

Haciendo ping a 192.168.2.20 con 32 bytes de datos:

Respuesta desde 192.168.2.20: bytes=32 tiempo=119ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=93ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=92ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=40ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=38ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=97ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=77ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=75ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=123ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=41ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=80ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=90ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=87ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=107ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=74ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=103ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=41ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=30ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=68ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=46ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=85ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=114ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=73ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=101ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=70ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=108ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=68ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=96ms TTL=126
Tiempo de espera agotado para esta solicitud.
Respuesta desde 192.168.2.20: bytes=32 tiempo=87ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=115ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=79ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=73ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=91ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=99ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=119ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=127ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=75ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=114ms TTL=126
Respuesta desde 192.168.2.20: bytes=32 tiempo=93ms TTL=126

Estadísticas de ping para 192.168.2.20:
    Paquetes: enviados = 40, recibidos = 39, perdidos = 1
    (2% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 30ms, Máximo = 127ms, Media = 84ms
```

Figura 77 Respuesta ping de PC de voz

Solo hay un paquete ping perdido, los tiempos de latencia siguen en aumento, pero el minino se encuentra en 30ms.

Sin embargo podemos observar a través de nTop que el servicio de video sigue siendo acaparando el canal:

Network Load	**Actual**	5.8 Mbit/s	555.5 Pkt/s
	Last Minute	6.3 Mbit/s	601.7 Pkt/s
	Last 5 Minutes	1.9 Mbit/s	187.3 Pkt/s
	Peak	6.5 Mbit/s	626.4 Pkt/s
	Average	2.6 Mbit/s	249.5 Pkt/s
Historical Data			[ ]

Figura 78 Tasa de transmisión para cuatro videos, con QoS CISCO

6.3 Con QoS de extremo a extremo.

El fin de hacer esta última prueba es por un lado observar que los servicios funcionen de manera correcta y por otro que se respeten las políticas de calidad. Por ello se cambió el uso de iPerf por un servidor de ftp.

El canal de video sólo transmitió un video bajo la limitación de no exceder 3.5 Mbps, el ftp se limitó a una tasa máxima de 100kbps, el canal de voz a 128 kbps, y el resto del canal se dejo libre.

Se capturó una imagen de video correspondiente a este servicio para comprobar su correcto funcionamiento cuando se emite una solo transmisión, posteriormente se intentó volver a saturar el enlace con emisiones paralelas de hasta 3 videos. Operando bajo estas condiciones se analizó la tasa alcanzada por el servicio de video, a su vez se descargó un archivo bajo el servicio de ftp donde el mismo servicio indicó la tasa de la descarga, y finalmente mediante pings se registró el comportamiento de los paquetes en el canal de voz, los resultados son los siguientes:

Imágenes:

Pantalla correspondiente a la emisión de un video:

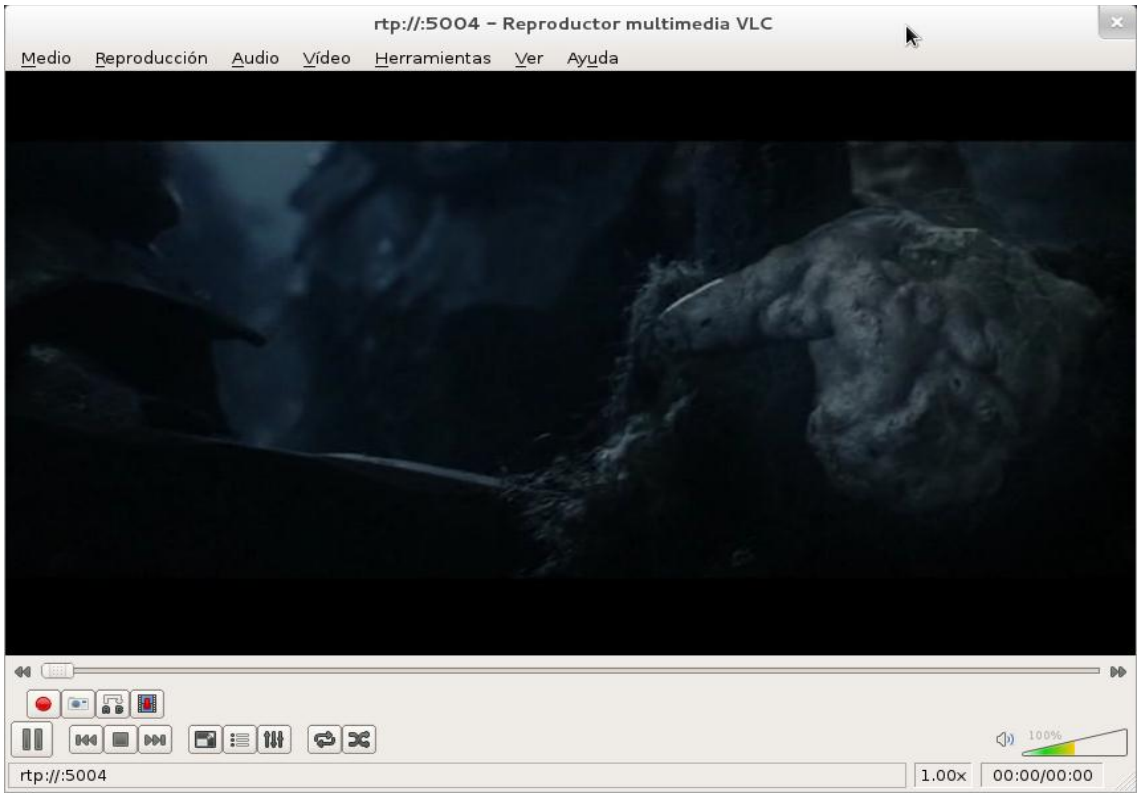


Figura 79 Imagen de un video transmitiéndose con QoS de extremo a extremo

Se prosiguió por emitir un segundo video de manera simultánea, la imagen correspondiente a la emisión de dos videos es:

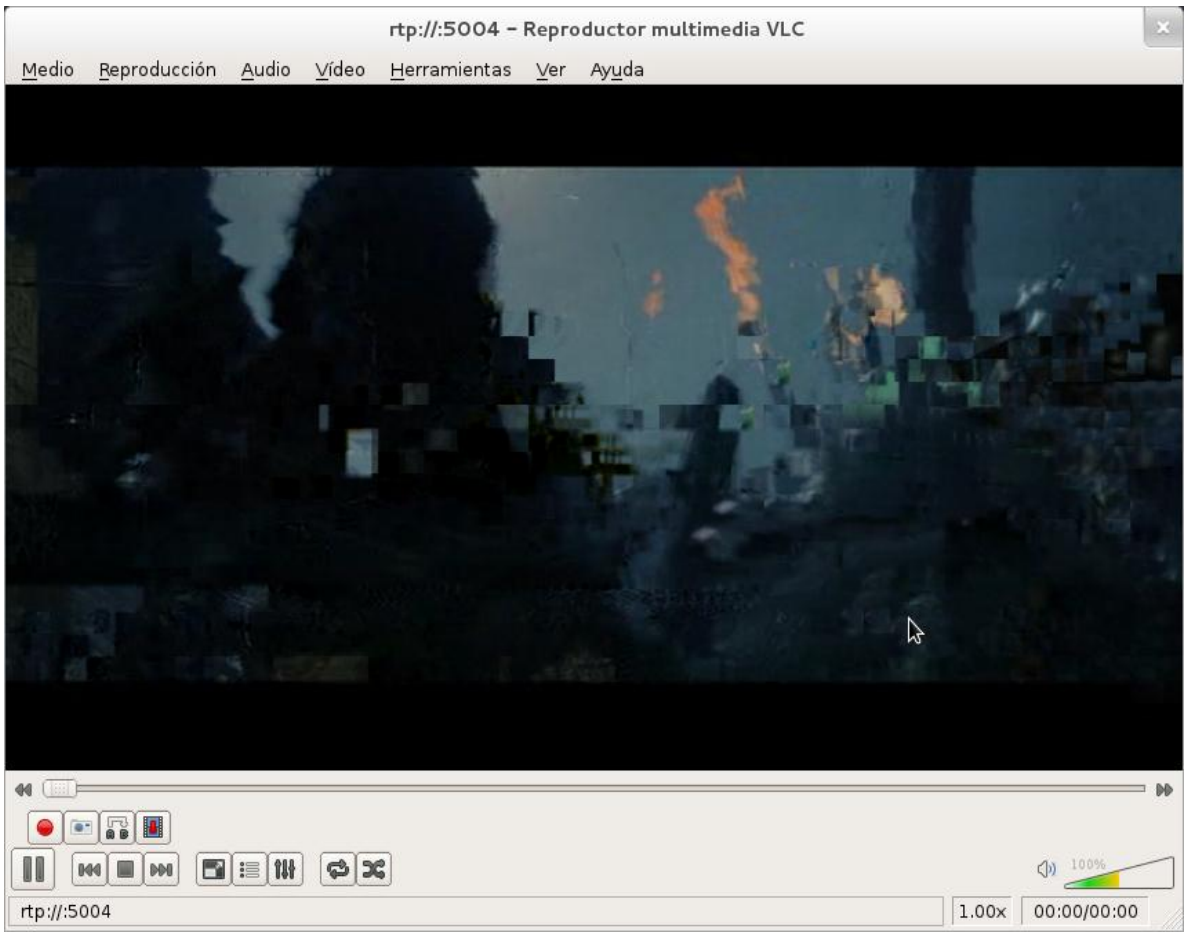


Figura 80 Imagen de dos videos transmitiéndose con QoS de extremo a extremo

Se continuó a emitir un tercer video, la imagen obtenida al hacerlo corresponde a la siguiente figura:

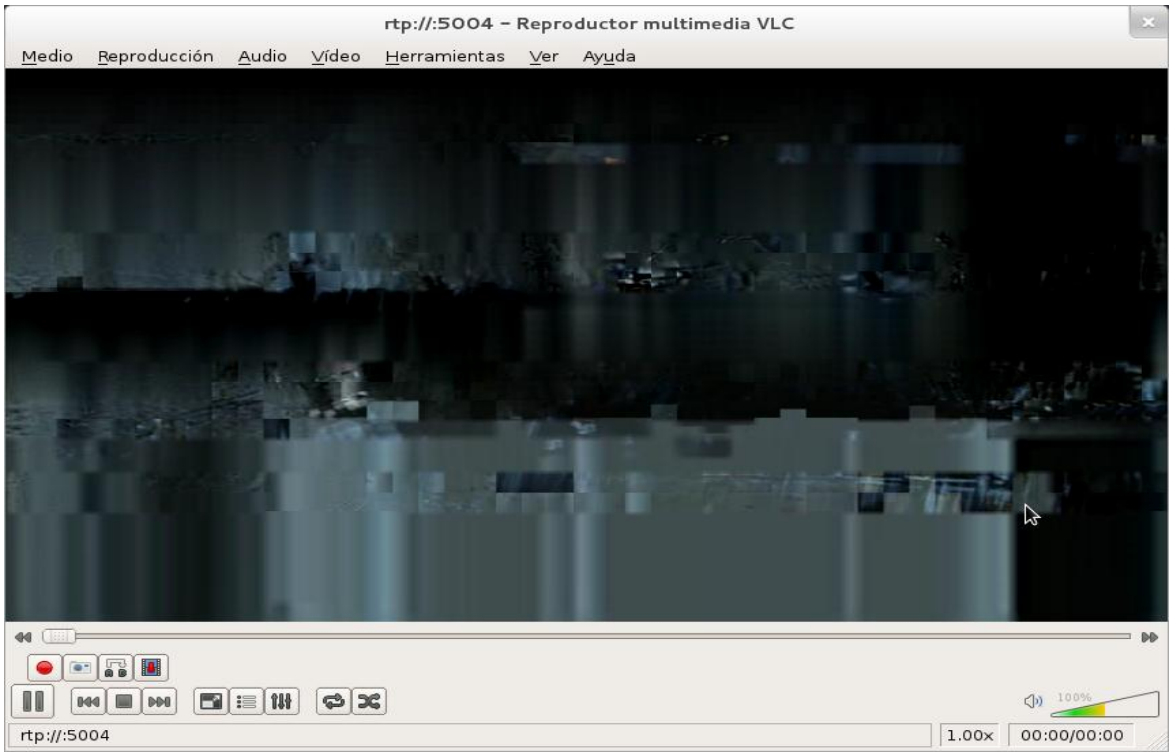


Figura 81 Imagen de tres video transmitiéndose con QoS de extremo a extremo

Antes de activar las políticas de QoS en la BS al transmitir tres videos pudo alcanzarse hasta 6 Mbps en el extremo del cliente de video, ahora los valores registrados para Ntop con tres videos fueron:

Network Load	**Actual**	3.3 Mbit/s	316.5 Pkt/s
	Last Minute	3.3 Mbit/s	317.6 Pkt/s
	Last 5 Minutes	3.3 Mbit/s	317.9 Pkt/s
	Peak	3.4 Mbit/s	324.6 Pkt/s
	Average	3.3 Mbit/s	316.8 Pkt/s
Historical Data			[ ]

Figura 82 Tasa de transmisión para tres videos con QoS de extremo a extremo

El uso de QoS en WiMAX mejoró significativamente el control sobre el tráfico de video.

6.3.1 Análisis 1. Retardo en el canal de voz

Primera prueba:

Ping 192.168.2.11 repeat 1000

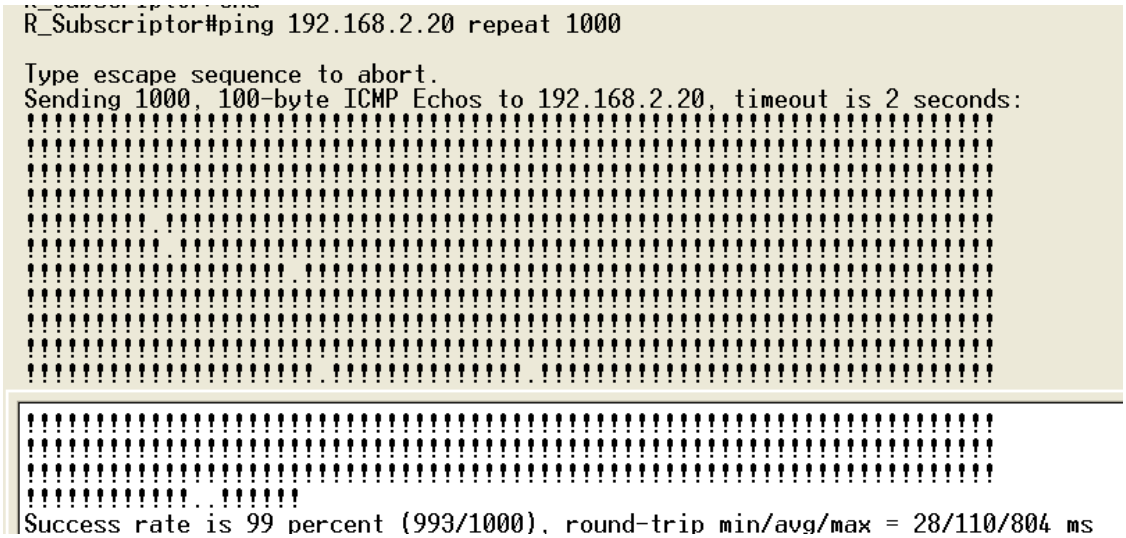


Figura 83 Respuesta ICMP del Router (ping repetido 1000)

Mejoro notablemente la respuesta de los mensajes ICMP, pero los retardos aumentaron mucho, el máximo estuvo en 804 ms

Segunda prueba

Ping 192.168.2.11 size 1000

Se crea un paquete ICMP de tamaño 1000

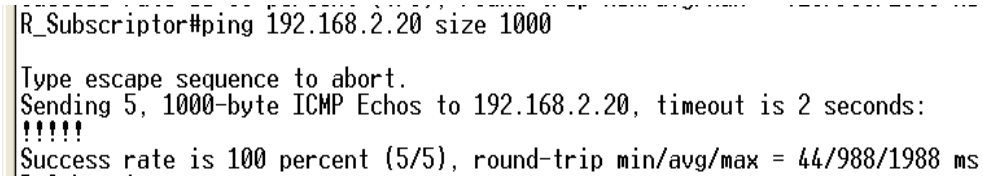


Figura 84 Respuesta ICMP del Router (tamaño paquete ICMP 1000)

Los paquetes ping fueron respondidos, pero la latencia sigue siendo alta, el máximo esta en 1988 ms.

Tercera prueba:

Se realizó un ping desde una computadora hacia otra computadora.

Se generó un ping que se repitió 40 veces.

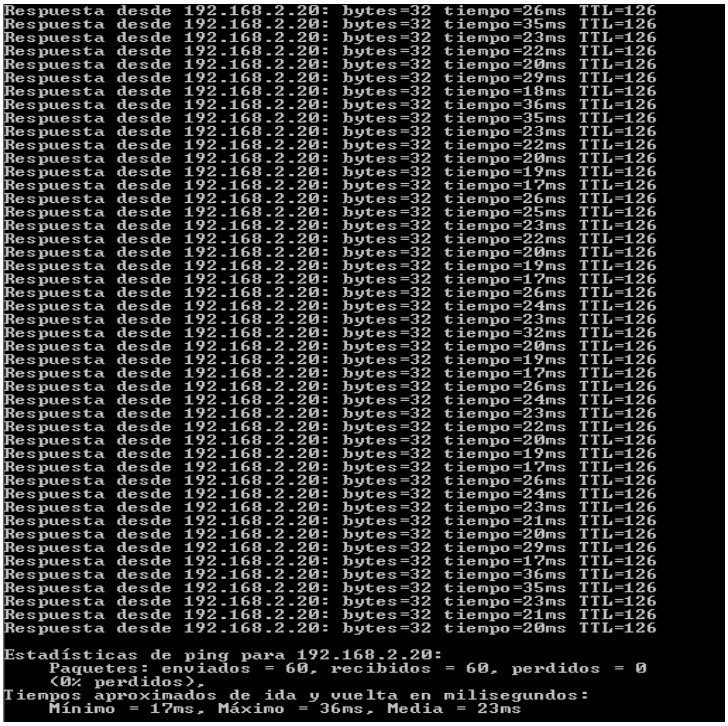


Figura 85 Respuesta ping de PC de voz

No hubo pérdidas en los mensajes ICMP, y los retardos fueron bajos, el máximo estuvo en 36 ms.

Respecto al canal de datos se realizó la descarga por ftp, la salida del cliente fue la siguiente:

```
[ulises@localhost ~]$ ftp 192.168.4.11
Connected to 192.168.4.11 (192.168.4.11).
220 (vsFTPd 2.3.4)
Name (192.168.4.11:ulises): ulises
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls -la
227 Entering Passive Mode (192,168,4,11,139,167).
150 Here comes the directory listing.
...
drwxr-xr-x    2 1000     1000         4096 Mar 13 03:46 Documentos
drwxr-xr-x    2 1000     1000         4096 Dec 29 22:58 Escritorio
-rw-rw-r--    1 1000     1000        38720 Mar 09 15:50 FormatosVideo.pdf
drwxr-xr-x    2 1000     1000         4096 Mar 23 02:16 Imágenes
...
226 Directory send OK.
ftp> get FormatosVideo.pdf
local: FormatosVideo.pdf remote: FormatosVideo.pdf
227 Entering Passive Mode (192,168,4,11,180,143).
150 Opening BINARY mode data connection for FormatosVideo.pdf (38720 bytes).
226 Transfer complete.
38720 bytes received in 2.75 secs (14.10 Kbytes/sec)
ftp> close
```

Figura 86 Resultados obtenidos en el cliente ftp

Donde realizando la conversión de la tasa de transmisión en Kbytes a kbits se tiene:

14.10 * 8 = 112 kbps

Comprobándose que FTP (un servicio TCP) pudo operar a una tasa similar a la reservada para su canal a la vez que se intentó saturar el enlace con múltiples videos, además el archivo descargado pudo abrirse sin errores.

CAPITULO VII

Conclusiones

En primer lugar comprobamos la ventaja de trabajar con servicios y equipos certificados bajo estándares de organismos de normalización. Tanto los servicios como los equipos empleados operan bajo el protocolo IP lo cual permitió el intercambio de información entre los hosts y a través de la red. Por otra parte las políticas de QoS se basan en el análisis del encabezado del paquete IP y del encabezado de las tramas MAC, de nueva cuenta estos operan bajo protocolos estandarizados lo que permitió que los equipos procesaran correctamente el flujo de datos.

Respecto a las políticas de QoS comprobamos que un enlace sin ninguna política definida conlleva a la degradación de todos los servicios cuando el canal es saturado. Además de implementarse políticas estas deben existir y coordinarse entre todos los dispositivos de red involucrados en el traslado, por ejemplo en las pruebas realizadas con QoS sólo en el equipo de CISCO se observó una pequeña mejora en el retardo de paquetes en el canal de voz, se redujo la pérdida de paquetes y el tráfico TCP pudo ser transmitido nuevamente; Sin embargo el tráfico UDP seguía consumiendo casi la totalidad del canal. Al usar en conjunto la QoS del equipo WiMAX y del equipo CISCO se obtuvo una mayor mejora en el

retardo y la pérdida de paquetes en el canal de voz, la velocidad de descarga en el canal de datos fue cercana a la deseada y la tasa de transmisión en el canal de video se contuvo exitosamente.

Finalmente comprobamos la importancia de los protocolos de la capa de transporte respecto a la saturación del canal. En principio intentamos saturar el canal mediante tráfico TCP pero este mediante los mecanismo de repuestas ACK y ventanas deslizantes ajustaba su velocidad de transmisión en función de la tasa libre en el canal, incluso disminuyéndola. En cambio UDP envía su información sin importar el estado de la red, ni siquiera el estado de la aplicación receptora.

ANEXO

GLOSARIO:

A

ADSL: Asymmetric digital subscriber line

AF: Assured Forwarding

ACL: Access control lists

B

BS: Base Station

BWA: Broadband wireless access

C

CF1: Identificador de formato ideal

cRTP: Compress RTP

CRC: Cyclic Redundancy Check

CBWFQ: Class Based Weighted Fair Queuing

D

DTP: protocolo de enlace troncal dinámico

DSCP: Differentiated Service Code Point

E

EF: Expedited Forwarding

F

FCS: Frame Check Sequence

FTP: File Transfer Protocol

H

HTTP: Hyper Text Transfer Protocol

I

ISP: Proveedor de servicios de Internet

L

LAN: Local Area Netework

LLQ: Low Latency Queuing

M

MGCP: Media Gateway Control Protocol

MQC: Modular QoS Command-Line Interface

N

NAT: Network Address Translation

P

PVID: ID de la VLAN de puerto predeterminada

PCM: Pulse Code Modulation

PHB: Per-Hop Behavior

R

RTP: Real-Time Transport Protocol

RTCP: Real-Time Control Protocol

RED: Random Early Detection

RSVP: Resource Reservation Protocol

S

SS: Suscriber Station

SCCP: Skinny Client Control Protoco

SIP: Session Initiation Protocol

SDP: Description Protocol

SDP: Session Description Protocol

SSH: Secure Shell

SNMP: Simple Network Management Protocol

T

TPID: valor de ID de protocolo de etiqueta

U

UDP: Protocolo de Datagrama de Usuario

UIT: Unión Internacional de Telecomunicaciones

V

VLAN: Virtual Local Area Network

VID: ID de la VLAN

Voip: Voice over Internet Protocol

VIC: Voice Interface Card

W

WAN: Wide Area Network

WiMAX: Worldwide Interoperability for Microwave Access

WRED: Weighted Random Early Detection

REFERENCIAS:

[1] Accesing the WAN, Cisco Networking Academy

[2] Redes de Computadoras, Andrew S Tanenbaum

[3] Network Fundamentals,Cisco Networking Academy

[4] Fundamentals of WiMAX understanding Broadband Wireless Networking

[5] IEEE 802.16-2004

[6] Sistemas de Comunicaciones Electrónicas, Wayne Tomasi

[7] Wireless Communications, Andreas F Molich

[8] Redline an-100u manual

[9] VLC usage documentation

[10] Redes. Manual de Referencia, Zacker

[11] Lan Switching and Wireless, Cisco Networking Academy

[12] CCNA Voice 640-461 Official Certification Guide Second Edition, Jeremy Cloara, Michael Valentine, September 2011.

[13] Recommendation ITU-T H.323: Packet-based multimedia communications systems.

[14] IETF RFC 3261, SIP: Session Initiation Protocol, published in June 2002.

[15] IETF RFC 2543, SIP: Session Initiation Protocol, published in March 1999.

[16] IETF RFC 3550, RTP: A Transport Protocol for Real-Time Applications, published in January 1996.

[17] Recommendation ITU-T G.711: Pulse code modulation (PCM) of voice frequencies.

[18] Recommendation ITU-T G.729: Coding of speech at 8 kbit/s using conjugatestructure algebraic-code –excited linear prediction (CS-ACELP)

[19] Redline SUI manual

[20] Routing Protocols and Concepts, Cisco Networking Academy

[21] Guía rápida para routers de la serie Cisco 2800 de servicios integrados LICENCIA Y GARANTÍA INCLUIDA, www.cisco.com

[22] Accessing the WAN, Cisco Networking Academy

[23] Data Sheet: Cisco SPA9000 Voice System, Cisco System

[24] Redes Cisco CCNP a Fondo. Guía de estudio para profesionales, ARIGANELLO, ERNESTO / BARRIENTOS SEVILLA, ENRIQUE

[25] Implementing Quality of Service Policies with DSCP, www.cisco.com

[26] Cisco IOS Quality of Service Solutions Command Reference, www.cisco.com

[27] Configuring Weighted Random Early Detection, www.cisco.com

[28] Vsftpd --help

[29] Iperf --help

[30] Ntop –help